NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SELECTION OF THE BEST SECURITY CONTROLS FOR RAPID DEVELOPMENT OF ENTERPRISE-LEVEL CYBER SECURITY

by

Oleksandr Tytarenko

March 2017

Thesis Advisor:	John Fulp
Co-Advisor:	Gurminder Singh

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE SELECTION OF THE BEST SECURITY CONTROLS FOR RAPID DEVELOPMENT OF ENTERPRISE-LEVEL CYBER SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Oleksandr Tytarenko	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

State-supported cyber attacks, cyber espionage campaigns, and hacktivist movements have forced many states to accelerate their cyber defense development in order to achieve at least a minimum level of protection against expanding threats of cyber space. As with any other development effort, cyber capability development requires resources of time, money, and people, which in most cases are very restricted. To rapidly build up "the first line of defense," enterprises should select the most efficient cyber controls and measures.

This thesis sought out the top 10–20 cyber security controls, where ranking was based upon a return on investment (ROI) assessment. This ROI assessment entailed consideration of both the likely/expected security benefits of each candidate security control (the "R" numerator), and the likely/expected cost associated with each security control (the "I" denominator). The primary references for security controls and their specifications are NIST Special Publication 800-53, revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and publications of SANS, NSA, ISACA, the Center of Protection of National Infrastructure, and other organizations dealing with cyber security. The selected security controls are presented in a standardized form, with sections for description, expected ownership cost, expected security provided, and general implementation recommendations.

14. SUBJECT TERMS cybersecurity, security controls, capability development, ROI, resource constraints	**15. NUMBER OF PAGES** 111
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

SELECTION OF THE BEST SECURITY CONTROLS FOR RAPID DEVELOPMENT OF ENTERPRISE-LEVEL CYBER SECURITY

Oleksandr Tytarenko
Major, Armed Forces of Ukraine, Army
M.S., Military Institute of Telecommunication and Informatization of the National Technical University of Ukraine "Kyiv Politechnic Institute," 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2017

Approved by: John Fulp
Thesis Advisor

Gurminder Singh
Co-Advisor

Peter Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

State-supported cyber attacks, cyber espionage campaigns, and hacktivist movements have forced many states to accelerate their cyber defense development in order to achieve at least a minimum level of protection against expanding threats of cyber space. As with any other development effort, cyber capability development requires resources of time, money, and people, which in most cases are very restricted. To rapidly build up "the first line of defense," enterprises should select the most efficient cyber controls and measures.

This thesis sought out the top 10–20 cyber security controls, where ranking was based upon a return on investment (ROI) assessment. This ROI assessment entailed consideration of both the likely/expected security benefits of each candidate security control (the "R" numerator), and the likely/expected cost associated with each security control (the "I" denominator). The primary references for security controls and their specifications are NIST Special Publication 800-53, revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and publications of SANS, NSA, ISACA, the Center of Protection of National Infrastructure, and other organizations dealing with cyber security. The selected security controls are presented in a standardized form, with sections for description, expected ownership cost, expected security provided, and general implementation recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. BACKGROUND 1
A. CYBER: THE FIFTH DOMAIN OF WARFARE 1
B. RISK MANAGEMENT FRAMEWORK (NIST SP 800–37) 6
1. Resource Constraints..9
2. Prioritization of Cyber Assets..9
C. RESEARCH APPROACH...11

II. CYBER SECURITY: UNDERLYING PRINCIPLES, FUNDAMENTALS AND BEST PRACTICES...13
A. DETERRENCE, PREVENTION, DETECTION, AND RECOVERY...13
1. Deterrence...13
2. Prevention...14
3. Detection 15
4. Recovery..16
B. CIA TRIAD 16
1. Confidentiality..16
2. Integrity 17
3. Availability..17
C. RISK EQUATION 18
D. REDUCING THE TARGET SURFACE AREA 19
E. PRINCIPLE OF LEAST PRIVILEGE 20
F. FAILURE TO AUTHENTICATE 21
G. REDUNDANCY AND CAPABILITY FOR RESILIENCY................22
H. ROI (RETURN ON INVESTMENT) EQUATION.............................24

III. CYBER SECURITY CONTROLS 27
A. NIST SP 800–53: AN INTRODUCTION 27
B. THE SECURITY CONTROL FAMILIES 28
C. ENVIRONMENTAL SPECIFICS 30
D. INDUSTRY RECOMMENDED STANDARDS 32

IV. SELECTION OF THE TOP SECURITY CONTROLS..................................37
A. RESTRICT USE OF ADMINISTRATIVE PRIVILEGES BY IMPLEMENTING GROUP SECURITY POLICY 37
1. Description...37
2. Justification 38

3. Recommendations 39

B. ENFORCE STRONG PASSWORD POLICY (USER ACCOUNTS AND EMAILS) BY IMPLEMENTING GROUP SECURITY POLICY 39

1. Description 39

2. Justification 40

3. Recommendations 41

C. ESTABLISH BASIC BOUNDARY DEFENSE BY DEPLOYING NETWORK INTRUSION PREVENTION SYSTEM 41

1. Description 42

2. Justification 42

3. Recommendations 44

D. DEVELOP BASIC RECOVERY CAPABILITY BY PERFORMING REGULAR BACKUP OF SERVERS 45

1. Description 45

2. Justification 45

3. Recommendations 47

E. MITIGATE GENERIC EXPLOIT TECHNIQUES BY DEPLOYING ENHANCED MITIGATION EXPERIENCE TOOLKIT 47

1. Description 48

2. Justification 48

3. Recommendations 50

F. ENHANCE END-POINT SECURITY BY DEPLOYING HOST INTRUSION PREVENTION SOLUTION 51

1. Description 51

2. Justification 51

3. Recommendations 52

G. CONTROL SOFTWARE EXECUTION BY IMPLEMENTING APPLICATION WHITELISTING 53

1. Description 53

2. Justification 54

3. Recommendations 56

H. ESTABLISH SYSTEMATIC OPERATING SYSTEM PATCHING BY DEPLOYING UPDATE SERVER 57

1. Description 57

2. Justification 57

3. Recommendations 59

I. PERFORM USER ACTIVITY MONITORING AND SYSTEMATIC AUDIT BY IMPLEMENTING GROUP SECURITY POLICIES....60

1. Description....60
2. Justification 60
3. Recommendations....62

J. PREVENT UNAUTHORIZED DEVICES FROM GETTING NETWORK ACCESS BY DEPLOYING AAA-SERVER 63

1. Description....63
2. Justification 63
3. Recommendations....65

K. ENHANCE BOUNDARY DEFENSE BY CONFIGURING ACCESS LISTS ON THE BORDER AND INNER ROUTERS....66

1. Description....66
2. Justification 67
3. Recommendations....69

L. IMPROVE INCIDENT RESPONSE CAPABILITY BY DEVELOPING INCIDENT HANDLING PROGRAM 70

1. Description....70
2. Justification 71
3. Recommendations....73

M. ESTABLISH SECURE CONFIGURED WORKSTATION BASELINES BY IMPLEMENTING SECURITY TECHNICAL IMPLEMENTATION GUIDES....74

1. Description....74
2. Justification 75
3. Recommendations....76

V. CONCLUSION AND FUTURE WORK 79

LIST OF REFERENCES....83

INITIAL DISTRIBUTION LIST....91

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Six Steps of the Risk Management Framework. Source: [24]. 8

Figure 2. Return on Investment Formula. Source: [36]. 24

Figure 3. The Effectiveness of 184 Exploits for Popular Applications on Windows XP, Windows XP with EMET Deployed, and Windows 7. Source: [73]..50

Figure 4. Windows 7 Vulnerability Overview. Source: [79]. 59

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. NIST 800–53 rev4 Security Control Families 28

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAA	authentication, authorization, and accounting
ACL	access control list
APT	advanced persistence threats
ASLR	address space layout randomization
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
DDoS	distributed denial-of-service
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNS	domain name server
DOD	The U.S. Department of Defense
DoS	denial-of-service
DTIC	Defense Technical Information Center
EMET	Enhanced mitigation experience toolkit
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
HIDS	host intrusion detection system
HIPS	host intrusion prevention system
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IS	information system
ISACA	Information Systems Audit and Control Association
IT	Information technology
NAC	network access control, network admission control
NAP	Network access protection
NATO	North Atlantic Treaty Organization
NIDS	network intrusion detection system

NIPS	network intrusion prevention system
NIST	National Institute of Standards and Technology
NSA IAD	Information Assurance Directorate of the National Security Agency
POLP	principle of least privilege
RADIUS	remote authentication dial-in user service
ROI	return on investment
SANS	System Administration, Networking, and Security Institute
SP	special publication
STIG	security technical implementation guides
TCO	total cost of ownership
UK NCSC	United Kingdom National Cyber Security Centre
U.S.-CERT	United States Computer Emergency Readiness Team
Water-ISAC SIC	Water Information Sharing and Analysis Center Security Information Center
WGP	Windows group policy

ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to my advisor, John Fulp, for his patience, motivation, and enthusiasm in guiding me to successful accomplishment. I am so very thankful for your time, guidance, and the numerous thought-provoking discussions we had. This research is the most valuable studying experience I have had while at NPS.

I would like to express my gratitude to Gurminder Singh and the faculty of the Computer Science department for the useful experience and knowledge I obtained.

My sincere thanks also go to Rebecca Pieken, Susan Hawthorne, Aileen Houston, and Meg Beresik for making this thesis readable.

I thank my fellow classmates, Khoubeib Bouthour and Alexis Peppas, for helping me with classes and always being supportive.

I also wish to dedicate this thesis to my loving wife, Hanna, for her love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. BACKGROUND

Cyber space has transformed from merely being a means of communication to that of being a key enabler of national security, economy, culture, and science. As with almost any other powerful tool, cyber space can be abused by those with malicious intentions. The unique features of cyber space, such as its virtual nature and its asymmetry of offense/defense aspects, provide advantages if used against opponents. State and non-state actors use various cyber related technologies against their opponents to achieve or support their military, political, religious, and economic goals.

Recent geopolitical changes and the transformation of the global security landscape have forced many countries and enterprise-level organizations to increase their efforts to mitigate constantly evolving cyber threats. From the defender's side, an appropriate cyber security framework is the starting point for all defensive efforts. Resource restrictions (e.g., budgets, human resources, time) require very careful selection of defensive approaches and their implementation.

Resource restrictions are the main motivator for this research. The goal of this thesis is to form a prioritized list of the most prudent and efficacious security controls that can most rapidly form a more robust "first line of defense." These controls should significantly enhance the cyber security of enterprise-level organizations that have insufficient resources for the more demanding comprehensive development of cyber security capabilities. The selection of controls is based on the return on investment (ROI) approach, which prioritizes solutions that provide the most security per unit of time, money, or human capital investment.

A. CYBER: THE FIFTH DOMAIN OF WARFARE

Leon E. Panetta, the U.S. Secretary of Defense in 2011–2013, during a speech in 2011 at the Woodrow Wilson Center said:

> Alongside this nuclear danger is an entirely new kind of threat we have to be better prepared to confront—the threat of cyber attacks. Cyber space has become a major concern as we face large numbers of attacks from non-state actors and large nations alike, and the prospect of a catastrophic

> disruption of critical infrastructure that would cripple our nation. The potential to paralyze this country from a cyberattack is very real. [1]

This quotation harmonizes well with the U.S. Department of Defense (DOD) attitude toward cyber space. DOD considers cyber space as the fifth warfare domain [2], adding to the four other well-known domains: land, air, sea, and space. Joint Publication 3–12 "Cyberspace Operations" defines cyber space as a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [3]. The success of virtually any modern military operation crucially relies on cyber space as the overall information infrastructure that provides the means for the military to gain and maintain a strategic advantage. Additionally, cyber space is a vital component of a country's overall economic prosperity and growth. The growing dependency on information technology and cyber space makes the various technologies that comprise them one of the biggest vulnerabilities of developed countries.

The vulnerabilities inherent in computer networks, along with highly sophisticated cyber attack techniques, present state and non-state actors with alluring opportunities to strike entire countries, including critical infrastructure targets. Executive Order 13636 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [4].

The Internet, the most prominent data exchange infrastructure that we use, was not originally designed to maximize security. Originally, it was an open system primarily intended to allow scientists and researchers to exchange data with one another quickly. Any military, medical, industrial, or other critical infrastructure system that connects to the Internet is a potential target for adversaries all around the globe. Despite all efforts to make cyber space more secure, it remains vulnerable to high precision, low cost, destructive attacks that can adversely affect an entire military operation, endanger millions of people, or collapse financial systems.

Cyber space is difficult to compare directly with the other four warfare domains, which are defined by their physical environment. The virtual nature of cyber space makes it borderless. Seán McGurk, Director of the National Cyber Security and Communications Integration Center with the U.S. Department of Homeland Security (DHS), has said: “There are no international borders and there [are] no oceans to cross” [5]. This distinctive feature of cyber space provides three unique benefits to an attacker: little likelihood of reprisal, inexpensive offensive capabilities, and asymmetry between offensive and defensive efforts.

Today’s cyber related means, approaches, techniques, and tools provide abilities to conduct cyber warfare operations against strategic targets with limited risk to the attacker. Attacker risk is limited, in part, owing to the difficulty in distinguishing between system failures that are the result of an accidental program or system error and those that are the result of intentional malicious activities (attacks). Furthermore, it can be very difficult to track the origin of attacks. Attackers can stay anonymous by operating from spoofed Internet protocol (IP) addresses and geographically distributed servers. They can also exploit compromised and remotely controlled computers to perform attacks with relative impunity.

The availability of relatively inexpensive offensive technologies provides attackers with means to rapidly create an offensive potential. No great investments are needed for development or usage of fairly advanced offensive cyber tools that can cause significant damage and disruption. These aspects of cyber warfare make cyber threats asymmetric. General Sir David Richards concludes this point by saying that “[at] relatively little cost, unsophisticated opponents with very cheap weaponry can pose a strategic threat” [6]. Attackers often need to find only one way to compromise a target; in contrast, defenders must contend with and defend all possible attack vectors. This exacerbates the asymmetry and requires high-cost solutions and investments by the defender. Moreover, defenders have to keep track of developing offensive methods in order to detect and mitigate newly developed attacks.

The National Institute of Standards and Technology (NIST) emphasizes that the threat space is expanding and “characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries” [7]. Tempo, in this context, can be characterized as “the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers” [7], according to NIST.

The division of cyber threat space, proposed by the British Chatham House report “On Cyber Warfare,” illustrates the variety of the malicious applications of cyber space. According to the report, cyber threats can be assigned to the following six main categories:

- direct military threats,
- indirect and non-military threats,
- terrorism and extremism,
- cyber espionage,
- economic cyber crime, and
- psychological cyber warfare. [8]

Non-state actors (e.g., terrorist organizations, cyber criminals, and hacktivists), as well as state secret services, have adopted cyber attacks and operations as effective tools to achieve political, economic, or military goals. Joint Publication 3–12 defines a nation state threat as “potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors” [3]. This publication also expresses the opinion that other nations can impose threats in the form of cyber attacks and cyber espionage. Furthermore, cyber espionage can come not only from adversaries but also from allies.

Past cyber attacks against Estonia, Georgia, Iran, and Ukraine serve as valuable examples of power projected via the cyber domain in order to achieve state goals or gain advantage in military operations. Russian-associated cyber attacks on Estonian network infrastructure in 2007 are the first publicly well-known example of a state-level cyber campaign. Dr. Olaf Theiler discusses how this case forced Estonia, and later all of the North Atlantic Treaty Organization (NATO), to reconsider the potential impact of cyber threats and the vulnerabilities of the cyber domain in general [9]. This paradigm shift resulted in the establishment of the NATO Cooperative Cyber Defense Center of Excellence in Tallinn.

The 2008 Russo-Georgian war is another milestone of conflict in the cyber domain. David M. Hollis in his study on this war says that it was the first known example of cyber attacks being well-coordinated and synchronized with major combat actions in the other warfighting domains [10]. About three weeks before the war began, multiple Russian hacker communities started to exploit vulnerabilities of the Georgian Internet infrastructure. With the first Russian troops crossing the border of Georgia, multi-vector cyber attacks disrupted government and private communications channels normally used by the Georgian authorities to communicate with their own people, as well as partner countries and other support organizations worldwide.

The next major historical milestone in offensive cyber activities was the deployment of Stuxnet, the malware designed specifically, according to the European Agency for Network Information Security's (ENISA) research, to target industrial control systems (ICS) [11] ICS remotely obtains sensor information from valves, pumps, transmitters, etc., and delivers proper control signals back *to* such devices. ENISA researchers indicate that the majority of infections were discovered within the Iranian telecommunication networks [11]. Nonetheless, the main target of Stuxnet was the uranium enrichment plant at Natanz that was involved in the state's nuclear program. According to Paul Mueller and other researchers, Stuxnet's interference with the plant's ICS resulted in the physical destruction of around 1,000 centrifuges at Natanz [12]. The Stuxnet case is considered by many security experts to be the first case involving usage of a cyber weapon and the most advanced malware seen on the world stage up to that time [13]. David Kushner, in [14], shows that the high level of sophistication, complex architecture, and the all-around research effort needed to develop it, are highly suggestive of state-level involvement.

Cyber warfare takes on special significance in the context of so-called hybrid war, as in, being an integral component *of* war. Hybrid, or non-linear, war is the combination of conventional warfare with economic, political, cultural, and cyber-oriented operations. The Russo-Ukrainian conflict, which started in 2014, is an example of various instruments of power applied through cyber space, such as propaganda, denial-of-service (DoS) attacks, website defacements, information leaks, and advanced cyber espionage campaigns. Russian special forces, using high-tech operations along with direct physical impact, disrupted strategic communication systems during the Crimea occupation in 2014.

During the operation in eastern Ukraine, Russian signals intelligence operations used intercepted-Internet data to locate and target Ukrainian troops. According to security researchers, to gather secrets from Ukrainian military and law enforcement officials, the Russian Federation has conducted several cyber espionage campaigns [15], [16]. David Sanger in [17] indicates that unrelenting cyber espionage campaigns have provided Moscow with considerable geopolitical and military advantage in the conflict with Ukraine. Snake, also known as Ouroboros or Turla, the cyber espionage malware comparable in its complexity to Stuxnet, has exfiltrated high value information from compromised Ukrainian government, diplomatic, and defense sector networks. The German security company GData, which analyzed the malware, concluded that it originated with Russian intelligence agencies that are part of the Russian government's cyber-weapons program [18]. Multiple pro-Russian hacker groups, as well as the Russian government, have interfered in the Ukrainian elections, attempted to block the Ukrainian government and news websites, and conducted various messaging campaigns against Ukrainian targets.

B. RISK MANAGEMENT FRAMEWORK (NIST SP 800–37)

Gijs M. de Vries, the European Union's anti-terrorism coordinator, has said: "We remain vulnerable. There is no such thing as 100 percent security" [19]. This quotation is well known among cyber security experts, knowing that achieving total cyber security of any organizational entity is an impossible task. This idea is a cornerstone of the risk-based approach to cyber security. Such an approach takes risk into account as the primary factor and considers effectiveness, efficiency, cost, and various legal/policy constraints in order to architect a balanced risk mitigation solution.

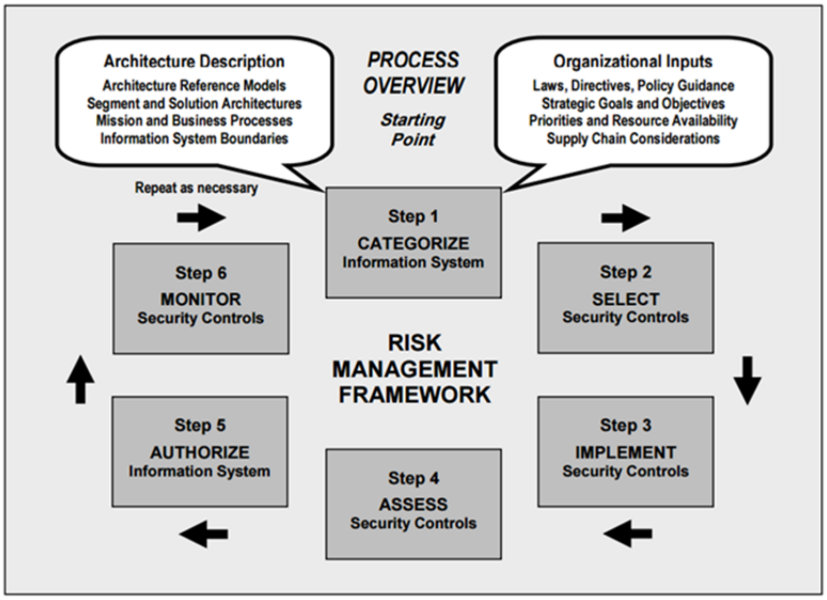
The complexity and constant evolution of cyber attacks require a consistent and iterative approach to identify, assess, and manage the risks associated with cyber security. In this context, according to FIPS–200, risk is considered as all potential threats "to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, and the Nation, due to the potential for unauthorized disclosure, disruption, modification, or destruction of information" [20]. The NIST SP 800–30 "Risk Management Guide for Information Technology Systems" defines risk management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level" [21].

The Global State of Information Security Survey 2016, conducted by PricewaterhouseCoopers, which covers various enterprise entities in 127 countries, shows that 91% of these entities have adopted risk-based security frameworks [22]. A framework is a baseline that identifies the main components of such an approach. A cyber security framework is a standard designed to assist with managing the confidentiality, integrity, and availability of data and critical infrastructure that, in part, depends on that data. The survey also indicates that as a result of applying this approach, these entities have been able "to identify and prioritize threats, quickly detect and mitigate risks and understand security gaps" [22]. A risk-based approach allows better collaboration of cyber security internal and external efforts, and helps to design, monitor, and measure cyber security activities.

The underlying idea is that attempts to apply *all* possible security controls to *every* IT-asset are impractical, if not impossible, and unsustainable. Resources spent on the protection of non-sensitive assets are not only inefficient, but diminish the overall security level, as cyber defense staff would likely be overwhelmed by numerous non-critical security incidents. Thus, understanding risk helps with the prioritization of cyber assets, shows what are the main protection concerns, provides guidance for better protection of systems and data, and helps determine what should (or should *not*) be invested to protect those assets. Jeff Jenkins in his article shows that the value of the risk-driven security approach ranges from financial savings (by concentrating security spending on the most sensitive assets) to loss mitigation (by keeping efforts primarily focused on responding to threats against critical assets) [23].

Various frameworks, such as: PCI DSS, ISO 27001, OCTAVE, FAIR, and U.S. CERT offer recommendations that are now in use in different counties and enterprise-level organizations. The Risk Management Framework developed by the NIST is one of the most widely known. This framework provides a structured and flexible way for managing the risks related to mission dependency on information systems. This framework presents a risk-based set of standards, security controls, specific details of risk assessment, and implementation of a mitigation strategy. It contains answers for typical questions and quick start guides that gather information from various NIST publications. The framework also provides simple ways to implement the standards and guidelines. According to NIST [24], broad-based concepts are used as a common language for addressing and managing cyber security risks.

As shown in Figure 1, this framework captures the concept of the security life cycle, based on six key activities in managing enterprise-level risk: categorize, select, implement, assess, authorize, and monitor. Each of these key activities is supported by associated NIST special publications. For instance Step 2, "Select," is covered in NIST SP 800–53 rev4 "Security and Privacy Controls for Federal Information Systems and Organizations." This publication provides a catalog of security controls for mitigating information system related risks, as well as recommendations on selecting controls [7]. The publication is a cornerstone of this thesis and is discussed in some detail in Chapter III.


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

The Risk Management Framework provides guidance on gradual planning and implementation of full cycle of risk management activities.

Figure 1. Six Steps of the Risk Management Framework. Source: [24].

1. Resource Constraints

Cyber development efforts and activities require appropriate resource allocation. The resource constraints mainly include financial constraints, timing constraints, and workforce constraints. Yet, in many cases the border between these constraints is not independent, as one often affects another. The financial constraints are the most influential one, as solving the other two constraints may be tremendously accelerated with increased funding. Manpower issues can be solved by using services of a third-party company. For instance, time needed to establish a core team of skilled cyber security experts may be decreased proportionally to the available financial resources. Nevertheless, increased financial resources cannot solve all resource constraints and limitations. For example, in some cases, especially those related to military missions, time is a crucial resource that cannot be substituted with other types of resources. Further, in many military applications, involvement of the third-party company is not an option due to classified information or combat situations.

According to “Security Market Trends and Predictions,” a survey conducted by the Institute of Information Security Professionals, 60% of enterprise-level cyber security budgets are insufficient to match the level of threats faced, and only 7% of respondents stated that security funds were increasing proportionally to, or faster than, cyber related threats [25]. Due to limited budgets and evolving cyber threats, cost-effective resource utilization that prioritizes the protection of the most crucial assets, while spending less on those assets deemed less crucial, is one of the most essential aspects of a cyber security development program. Such an approach requires a risk-based selection process to identify the cyber security controls likely to deliver the greatest security ROI.

2. Prioritization of Cyber Assets

Cyber assets are “programmable electronic devices, including the hardware, software, and data in those devices” [26], as defined in the glossary of terms used by the North American Electric Reliability Corporation. To efficiently use available resources in order to protect its most critical assets, an enterprise-level organization should perform a prioritization analysis. For instance, network components, data, and processes need to be prioritized based on their criticality in support of accomplishing mission objectives. According to the DOD Cyber Strategy, assessment of risks and hazards and careful prioritization of the systems and data to protect is a crucial responsibility of governments, companies, and organizations [2].

Risk assessments combined with an understanding of risk tolerance can help enterprise-level organizations prioritize cyber security activities. To achieve this, they have to establish priorities and make decisions through a process of evaluating the operational value of data, its sensitivity, possibility of threats, and vulnerability assessment of systems components. Besides that, clear identification by cyber defense operators of cyber assets critical to support mission priorities is a key to successful defense against an overwhelming number of cyber threats. Defenders have to decide and act quickly. With overwhelming threats, triage and prioritization should be performed in order to make decisions on the response technique to use. As described in a Naval Research Laboratory paper, “A Framework for Event Prioritization in Cyber Network Defense,” cyber incidents and security events should be triaged based on the potential damage they have to important assets and the mission [27]. This enables a better protection of critical missions by focusing on high priority events.

The prioritization of cyber assets and cyber effort is the cornerstone of rapid cyber defense development. Rapid development of cyber capabilities is called for when a particular organization’s level of cyber security readiness is deemed far less than desired, and when an organization faces constraints in resources (financial, time, manpower), a systematic approach cannot be used to incrementally build up the cyber security program over a longer time frame. With a constantly expanding cyber threat space, along with rapidly changing geopolitical and global financial situations, some enterprise-level organizations, even entire nations, face new cyber-based threats for which they are ill prepared.

Even though there is a general trend of increasing cyber security efforts, parts of this description, with some level of certainty, can be applied to many enterprise-level organizations, governmental organizations, and global business entities. According to the “2015 Global Cybersecurity Status Report,” issued by the Information Systems Audit and

Control Association (ISACA), only 38% of responders stated that they consider themselves ready for sophisticated cyber attacks, and 86% answered positively to the question “Do you believe there is a shortage of skilled cyber security professionals?” [28]. Another research report, the “2015 Cyberthreat Defense Report,” showed that only 23% of respondents were confident that their organizations had made adequate investments in the tools needed to properly monitor their various information technology (IT) systems for indications of attack or compromise [29]. For such cases of insufficient resources available, careful prioritization of efforts and efficient utilization of constrained resources is the only option to protect valuable assets.

C. RESEARCH APPROACH

To answer the research question, this work is organized into five chapters. Chapter I provides the introductory information regarding this thesis and its goal. Chapter II introduces the underlying principles, fundamentals, and best practices involved in cyber security. It prepares readers who are unfamiliar with the topic for later discussion regarding security controls. Chapter III describes the approaches, structure, and security control families as defined by NIST’s Special Publication (SP) 800–53 rev4. Chapter IV focuses on forming a prioritized list of the security controls deemed to provide the most ROI for rapid cyber security development. Each chosen security control is briefly described, and then the rationale is offered for why it was chosen. Chapter V is the conclusion. It summarizes the work done and offers suggestions regarding future, follow-on work related to this research.

There are several frameworks, standards, and guidelines covering measures to implement in order to increase the level of cyber security. They represent different approaches and classifications of this measure and corresponding security controls; however, all have in common a systematic approach for obtaining and strengthening cyber security capabilities. This approach has proved its effectiveness through the years, but it requires the allocation of appropriate resources, which, as discussed earlier, is not always possible. To establish an initial, yet significant, line of cyber defense, it is necessary to prioritize and implement ROI principles.

This research selects those technical or organizational cyber security controls most suitable (i.e., maximum "R" per invested "I") for rapid development of cyber defense capabilities with limited resources. The main focus is on analyzing existing security controls to determine the investments needed to implement new or enhanced cyber defense capabilities, along with the expected security benefits of their implementation. This thesis involves the study of the main principles and techniques of cyber security, such as the CIA triad (Confidentiality, Integrity, and Availability), the principle of least privilege, risk management, the risk equation, return on investment, and other "pillars" of cyber security.

The main effort of this thesis is to analyze existing governmental and private sector guidelines or standards that specify measures and technologies intended to mitigate cyber threats. The main focus is on security controls. The main criteria to be considered are the extent of the expected investment and the expected result (or return) on an organization's cyber security posture after a particular control is incorporated. The primary reference for security controls and their specifications is NIST SP 800–53 rev4 "Security and Privacy Controls for Federal Information Systems and Organizations."

II. CYBER SECURITY: UNDERLYING PRINCIPLES, FUNDAMENTALS AND BEST PRACTICES

A. DETERRENCE, PREVENTION, DETECTION, AND RECOVERY

James LaPiedra, from the System Administration, Networking, and Security Institute (SANS), describes information security as a “process that goes through phases, building and strengthening itself along the way. Security is a journey not a destination” [30]. All the various tools used to achieve cyber security can be grouped according to where the functionality of each fits into the defense continuum—deterrence, prevention, detection and recovery. The idea of deterrence is to discourage a potential attacker from even initiating an attack. When deterrence fails, prevention is the next best outcome of an attempted attack. When prevention fails, detection is essential in order to inform the affected system owner of its occurrence. And last, recovery takes over once detection has occurred, and its activities will seek to restore the normal state of the system. None of these can guarantee that an attacker will not succeed in causing some form of damage to the targeted system; however, each of them can reduce the number of successful breaches and reduce the severity of those that do initially succeed in causing some level of damage. All four serve as a manageable cyber defense cycle, providing the high-level framework for dealing with ongoing cyber attacks.

1. Deterrence

Richard L. Kugler, a well-regarded security analyst, in his work “Deterrence of Cyber Attacks” demonstrates that deterrence as a concept of a traditional security theory can be imposed on the cyber domain [31]. Deterrence is aimed at discouraging potential attackers or policy violators from intentional harmful actions against the system to be protected. Deterrence is realized as specially designed constraints that raise the quantity of resources needed, time, and the level of expertise needed to perform malicious activity. These constraints make a potential attack too difficult or undesirable. Also deterrence might be implemented in the form of threat of consequences or potential punishment to a violator. All forms of deterrence should influence a potential intruder to give up and not perform malicious activities because the cost or consequences of an attack outweigh its desired benefits.

Thus, any deterrence efforts should include two components. The first one is the implementation of effective defensive mechanisms that make malicious activities exceedingly difficult. The second component is that of ensuring retaliation for any performed attack. This theory was effectively implemented during the Cold War in the form of nuclear deterrence. The defensive component was embodied in the deployment of sophisticated anti-missile systems. Precise high-orbit satellites and a variety of nuclear delivery systems facilitated the retaliation capability/threat. In contrast with nuclear deterrence, the cyber realm version of deterrence is somewhat more problematic. The anonymous nature of the digital domain results in difficulties and uncertainties of identifying the source of a cyber attack.

2. Prevention

Prevention aims at blocking malicious activities in their delivery phase, thus preventing them from actually causing the intended effects/harm. It is preferable to prevent an incident rather than to detect and recover from one. The key idea of prevention is modification of a computer system or environment in order to minimize potential ways of conducting a cyber attack against this system.

Establishing reliable prevention mechanisms requires deep system analysis and careful planning. The planning should consider both accidental and intentional unauthorized modification, destruction, and disclosure of the information stored, processed, or transmitted by the system. Prevention is based on establishing and properly implementing security policies, controls, and processes. The incident prevention policy is the basis on which technical and administrative measures are built. Technical measures and controls could be either automated or manual, depending on the security policy and available resources for implementation of the policy.

When preventive controls are implemented, the implementer must carefully consider tradeoffs regarding security and usability. Too much prevention can result in reduced user productivity, whereas too little prevention can result in system compromises. The *Information Security Management Handbook* states that an effective user awareness program helps to increase users' tolerance for restrictions posed by preventive controls [32].

3. Detection

Detection of a security incident or policy violation is extremely important when deterrence and prevention controls do not stop an attacker. The last two are not very effective against so-called advanced persistence threats (APT). APTs can be characterized with a high level of attacker motivation, skills, and resources. APTs can exploit human factors using methods of social engineering that can bypass technical defensive measures. Thus, a system should be considered as likely vulnerable to APT. Not only APTs but other new or evolving threats can defeat existing preventive controls. Thus, reliable detection mechanisms should ensure that when defensive measures fail, the indications of the incident will be identified in timely manner so that appropriate response actions can be taken.

The NIST "Guide to Intrusion Detection and Prevention Systems (IDPS)" defines an intrusion detection capability as "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents" [33]. Intrusion detection systems (IDS) sensors are usually deployed in various locations within a network to provide passive monitoring and threat identification based on signatures of known exploits. IDSs inform security personnel when intrusion attempts are detected. To distinguish normal system activity from malicious activity, IDSs should be properly configured and adjusted to each individual network or system.

IDSs are usually categorized into two broad groups: network-based IDSs (NIDS) and host-based IDSs (HIDS). NIDS monitor traffic and events that occur via packets transiting between various devices on the network. HIDS monitor events and application activity in the computer system (host) on which it is installed. HIDS, in most cases, is implemented as a software agent on the host operating system.

4. Recovery

Recovery controls form mechanisms that ensure availability of all resources needed to restore lost computing resources, capabilities, and services caused by a cyber incident. Such controls should address the major types of incidents, such as intentional malicious activity, unintentional security policy violation, and natural disasters. Recovery is based on procedures, techniques, and the appropriate tools that enable rapid backup and restoration of a computer system so as to minimize potential losses.

At some stage, the recovery process should remedy the root vulnerability that enabled the incident in the first place. Execution of such corrective remediation may entail changes to current administrative or technical controls and will, ideally, prevent similarly targeted incidents from happening again. Analysis of incident root causes and the various ways to address them are the two main components of any post-incident report. This process is an important part of strengthening an organization's overall cyber security posture. With new information regarding the root causes of each incident included in post-incident reporting, security personnel may leverage this to improve the quality of preventive security controls that may have missed attack indicators the first time around. In this manner, recovery efforts begin to overlap with prevention activities, which illustrate the cyclic nature of deterrence, prevention, detection, and recovery efforts.

B. CIA TRIAD

Information security policy within an organization has as its ultimate goal protection of three unique information attributes: confidentiality, integrity, and availability. These attributes are also known as the "CIA triad," considered as the most important conceptual model of information security and cyber security.

1. Confidentiality

The Federal Information Security Management Act of 2002 (FISMA) defines confidentiality as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"

[34]. This means that information should only be seen by authorized entities. Loss of confidentiality is a result of the unauthorized disclosure of information.

In computer systems, data encryption is a widely used approach for protecting confidentiality. Authentication, followed by authorization, is the standard procedure for implementing security controls intended to provide the information security objective of confidentiality. These procedures include user authentication based on biometrics, private knowledge, or knowledge/possession of secrets (e.g., passwords). As additional precautionary measures, system designers should strive to minimize the exposure of sensitive information by constraining it to appropriately secured devices, networks, and cryptographic mechanisms.

2. Integrity

Integrity is defined as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" [34]. Through the entire life cycle of information, steps must be taken to insulate information from unauthorized modification or destruction as they result in a loss of integrity. Gopalan Sivathanu from Stony Brook University classifies integrity violations in three groups: hardware and software errors, malicious intrusions, and inadvertent user errors [35]. Measures taken to ensure the integrity of information and information systems maintain the trustworthiness and accuracy of data. This information security objective can be achieved using encrypted checksums. Various types of data backup schemes can restore the correct information state in case of a data compromise and, in this way, help to maintain the integrity of the data.

3. Availability

The third critical information security objective is availability. According to FISMA, availability is defined as "ensuring timely and reliable access to data and use of information" [34]. FISMA also indicates that "the disruption of access to or use of information or an information system" [34] results in a loss of availability. Methods to maintain availability include consistent hardware maintenance and performing necessary system upgrades, for both hardware and software. High-availability clusters and hardware redundancy can minimize losses caused by hardware failures. Occurrences of communication bottlenecks can be mitigated by providing more bandwidth and having reserve backbone connections for use when main channels are at full capacity. Geographically isolated backup storage and service providing facilities can help to maintain availability in case of natural disasters such us floods, fires, or tornados. However, since attackers have myriad ways to break correct functional processes, availability is the most difficult security objective to guarantee.

C. RISK EQUATION

As has been addressed previously, risk management is the key managerial activity needed to ensure security resources are applied in the most efficacious manner, taking into account relative measures of risk and economic constraints. It establishes a common approach to identify and assess potential threats and vulnerabilities. It provides ways to determine what measures are needed for minimizing or avoiding the identified risk. Misunderstanding of risk, or its uncertainty, can lead to negative consequences and prevent the application of effective and efficient mitigation measures.

The Risk equation is a tool used to determine risk. The equation describes the relation of four basic security concepts: vulnerability, impact, threat, and security controls. Risk can be described as the probability that a threat will exploit a vulnerability to cause negative impact to the system or an asset. This probability can be mitigated by security controls. Naval Postgraduate School Senior Lecturer John Fulp provides the following risk equation that is commonly used in cyber security:

Risk = (Threat x Vulnerability x Impact) / Security controls [36].

As we can see from the equation, if any one of the three components in the numerator is zero, then the risk “product” is also zero. For instance, if there is no threat, then there is no risk, even if high potential impact and severe vulnerabilities exist in the system. Thus, risk appears when there are at least some of each: threat, vulnerability, and impact.

Unfortunately, the world we inhabit and, particularly, the cyber systems we operate are rife with targeted threats and innate vulnerabilities; thus, risk is a constant reality. The general idea of risk management is to determine potential risk, and then reduce it to an acceptable level. In this perspective, cyber security efforts are focused on both removing vulnerabilities and applying security controls. Well planned and implemented security policies, procedures, and technical solutions can effectively mitigate risk. Defensive efforts also should be aimed at the reduction of vulnerabilities by performing systematic vulnerability assessments and applying fixes and patches in a timely manner.

D. REDUCING THE TARGET SURFACE AREA

"Attack surface" is very important concept of cyber security that, when understood, can be leveraged to reduce the likelihood that cyber attacks are successful. According to Pratyusa K. Manadhata from the Institute of Electrical and Electronics Engineers (IEEE), a system's attack surface can be defined as "the set of ways in which an adversary can enter the system and potentially cause damage" [37]. In other words, it is the sum of all vulnerabilities that can potentially be exploited. Most cyber attacks start by scanning the targeted system in order to discover potential attack vectors. Intuitively then, minimization of the attack surface via elimination or reduction of such vulnerabilities and vectors will reduce the exposed risk of the system.

The principal idea behind this concept is the precept that one should enable only that minimum system functionality truly necessary for mission accomplishment. Any additionally enabled functionality would, according to this concept, only increase the opportunities of attacker success. The first step in reducing the attack surface area is an improved understanding of one's network and the various devices and programs running within it. Clear understanding of the network architecture, the purpose of all hosted assets, along with their condition and status, is a necessary starting point for reduction of the attack surface area. All of these efforts, as well as other steps taken to implement the least privilege principle, help reduce the "attack surface area" of the system. The *CompTIA Study Guide* explains that the least privilege principle can reduce the attack surface by “eliminating unnecessary privileges that can result in network exploits and computer compromises” [38].

E. PRINCIPLE OF LEAST PRIVILEGE

“Least privilege” is a foundational principle for cyber security. The principle of least privilege (POLP) represents the practice of providing the least authority/access necessary to achieve any required and authorized functionality. NIST SP 800–14 “Generally Accepted Principles and Practices for Securing Information Technology Systems” describes the principle as follows: “least privilege refers to the security objective of granting users only those accesses they need to perform their official duties” [39]. The principle aims to improve security by limiting the potential negative consequences of a security breach (intentional, accident, or error). Least privilege is well-known in military circles under the very similar “need-to-know” concept, where users are not granted access to sensitive information for which they have no mission-related need. Gary McGraw in [40] adds that the least privilege principle also suggests limiting the time for any granted access to the minimum necessary. The United States Computer Emergency Response Team (US-CERT) observes that careful selection and delegation of access rights can reduce the number of possible avenues of attacks [41]. “Least privilege” and the corresponding implementations of sufficiently granular access decisions require reliable authentication mechanisms. Such mechanisms will ensure that entities requesting access to resources are truly who, or what, they are presenting themselves to be. A common example of this is a person attempting to execute a privileged system command that is reserved only for system administrators. Without a reliable authentication mechanism, anyone—not just system administrators—would be able to execute privileged commands.

Reliable authentication also enables system-wide auditing, where important actions can be attributed to the person or other entity (e.g., system-to-system actions) that initiated them. Such an audit/attribution mechanism should maintain a one-to-one correspondence between the actor/entity and whatever manner of identifier is used to represent him/her/it in the system.

Privileged access rights should be granted to a very small group, and this group should be subjected to more strict auditing/accountability standards owing to the added severity of damage that their higher privileges facilitate. Furthermore, administrators should use their privileged accounts only for tasks that require higher level permissions. All other routine, non-critical tasks, like web-browsing or email access, should be done using less privileged user accounts.

The separation of duties helps reduce the consequences of malware infection, some networks attacks, and other security incidents. Malware, when activated on a system, usually runs with the privileges of the user who activated it. Thus, the malware activities initiated under a normal user account have less destructive potential than the same malware launched with administrator privileges. This simple but effective approach ensures that the impact of an account being compromised will be minimized by the limited privileges granted to this account.

A firewall is, perhaps, the most visible example of a security device (whether hardware- or software-based) that can implement a form of "least privilege." In this regard, SANS notes that firewall rules should be configured to permit only communication that is required for the proper functioning of permitted services and applications [42]. For example, such a rule allows only mail-server protocol traffic (e.g., POP3, IMAP, and SMTP) to traverse through the firewall to a public mail server.

Another example of applying "least privilege" is seen in server, host, and operating system "hardening." Hardened systems should use only system services that are required for normal operation; all other services have to be disabled. Disabling unneeded services reduces the number of possible attack vectors and vulnerabilities that can potentially be exploited. Another aspect of hardening is that of disabling unused user accounts.

F. FAILURE TO AUTHENTICATE

One of the fundamental benefits of the Internet is the delivery of data from almost any source to almost any destination, without any requirement to validate the authenticity of the source. This approach makes the Internet, as we know it, fast, smooth, and easy to use. From the other side, however, the lack of source authentication results in a vulnerability that can be taken advantage of by attackers. US-CERT describes a domain name server (DNS) amplification attack as a popular form of distributed DoS attack (DDoS), which exploits the failure to authenticate [43]. The attack is based on an open DNS server that resolves any request it gets without validating the requester's IP address. John Fulp explains the flow of the attack as follows: to perform the attack an attacker sends to an open DNS server a specially crafted DNS query request that has its IP source address spoofed to match that of the victim's IP address [44]. The attacker can easily send a large, and continuous, volume of such spoofed DNS requests, so as to flood the victim's network bandwidth. In this way the attacker uses vulnerabilities of DNS protocols and turns small protocol queries into large amplified responses that can exhaust the victim's resources and cause the denial of service. The mitigation of failure to authenticate is obviously the implementation of a reliable authentication mechanism.

G. REDUNDANCY AND CAPABILITY FOR RESILIENCY

Resilience is the ability of a system to maintain an acceptable level of service when faced with various challenges and faults. David Tipper says that the objective of resiliency is to avoid failures, a situation where the network is unable to deliver acceptable quality of communication services [45]. In networking, these services provide the ability for users to access information when needed.

The ENISA differentiates four main challenges that can be obstacles to achieving resiliency:

- *Infrastructure* formed by all hardware and software assets that enable network communication, functionality, and operations of computer systems, power, and other supportive facilities.
- *Technology platforms* represented by protocols, hardware, and software implementations.
- *Organizational process*. Process here includes but is not limited to network management, configuration management, incident response, etc.
- *Organizational continuity* includes resources for continuity and resilience, technical training, user awareness, crisis communication, and so on. [46]

A well-known example of a technology platform challenge would be a DoS attack that exploits finite resources of a computer system. DoS and DDoS attacks can paralyze entire systems by sending an overwhelming volume of requests that eventually exhaust the targeted resource. Resources in computer systems can be divided into three broad categories: memory, bandwidth, and processing. Bandwidth DDoS attacks overload a communication channel such that no bandwidth is left for legitimate communications. This can be done by a bot-net network comprised from many devices (“bots”) connected to the Internet and covertly controlled by a “master.” When “masters” control hundreds or thousands of “bots,” they are capable of constantly sending a large number of apparently legitimate packets to targeted routers, servers, and firewalls. All these targeted devices are connected to the Internet by channels with limited bandwidth, and by themselves, have limited processing resources and memory with which to deal with the large volume of traffic/requests. A Riverhead Networks Whitepaper discusses how as a result of such packet-flooding attacks, targets fail under the excessive load and can no longer process valid transactions [47]. In a military environment, even a short-term disruption in communication services can jeopardize a mission and result in loss of human life. In the business sector, such service failures can result in frustrated customers and high financial loses.

On October 21, 2016, a powerful DDoS attack against one of the biggest network service providers in the United States caused PayPal, Twitter, Amazon, Reddit, Tumblr, Netflix, and more than a hundred other popular websites to be unreachable for several hours. Steve Evans in his article indicates that this attack disrupted the functionality of Internet-based services along the U.S. West Coast and affected millions of users [48]. Famous security technologist Bruce Schneier made a comment on this attack: “the size and scale of these probes—and especially their persistence—points to state actors. It feels like a nation’s military cyber command trying to calibrate its weaponry in the case of cyberwar” [49]. This is an illustrative example of the utilization of cyber attacks on a large scale against nation-level infrastructures.

Cisco explains that the finite nature of system resources, along with the distributed sources of DDoS attacks and easily available DoS tools, makes DDoS attacks very difficult to defend against [50]. There are various defense methods against various attack methods. Protective devices that perform signature matching detection of attacks are not very effective against DDoS attacks, as it is difficult to distinguish packets that come from a "bot" from those that come from a legitimate user. Another DDoS defense approach uses anomaly-based monitoring to detect unusually high volumes of traffic coming from a single origin. However, such defensive mechanisms can be eluded by IP-spoofing, "a type of impersonation technique, where the attacker transmits packets with a forged source IP address rather than its own" [51]. The easiest, although expensive, way to defend a system against DDoS attacks is to have redundancy in the resources the system uses. Since a denial of service attack is largely an attack against capacity, having additional capacity is one way to mitigate disruption in services. Provisioning excess bandwidth or having redundant network devices can help to handle extreme surges in request demands and mitigate the effects of an attack.

H. ROI (RETURN ON INVESTMENT) EQUATION

The Informing Science Institute describes return on investment (or ROI) as "one of the most popular performance measurement and evaluation metrics used for evaluating existing information systems and making informed decisions on software acquisitions and other projects" [52]. The computer security world sometimes uses the related term, return on security investment, instead. The metrics are used for evaluating potential investments in security solutions in order to compare them and choose those that "deliver the most for the least." The solution with the highest ROI is prioritized. John Fulp expresses [36] the return on investment in the formula (Figure 2):

$$\mathrm{ROI} = \frac{\text{ExpectedLossBefore}^{*} - \text{ExpectedLossAfter}^{*} - \text{CostOf\_Sec\_Control}}{\text{ExpectedLossBefore}^{*}}$$

* Relative to application of the security_control

Figure 2. Return on Investment Formula. Source: [36].

Application of ROI in business and security varies and includes: justification of potential investments and acquisition decisions, security solution prioritization, evaluation of existing solutions and their post-implementation assessments. Cyber security tools do not produce a tangible profit; they are designed to prevent incidents. Therefore, return on security investment may be interpreted as a profit that comes from saving money that would be spent on overcoming negative consequences of any or all realized incidents. However, in cyber security, there exists a myriad of additional probabilistic factors that further complicate anything resembling a precise valuation of return (i.e., the "R") in the ROI calculus.

Quantitative calculation of return on investment is a usual business practice. In cyber security, however, the quantitative approach becomes too complex, sometimes controversial, and often difficult to understand. For example, most automated security solutions may require a certain amount of configuration and adjustments. Such customization work can cost many times more than the cost of the initial purchase of the non-configured tool itself. Furthermore, in order to function properly, many cyber security tools require some kind of subscription or licensing for technical support, updates, signatures, and online services. These factors also add a lot of uncertainty to the "I" of the ROI calculus. Loss is another factor of uncertainty and guessing. In light of constantly evolving threats, rapid development of cyber offensive capabilities can change the security landscape tremendously in a short amount of time. What is thought secure today, may not tomorrow. In cyber security, ROI can, however, be effectively used in a *qualitative* manner. For instance, the IT industry widely uses several methods, notably:

- the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE);
- NIST SP 800–30 rev1 "Guide for Conducting Risk Assessments"; and
- Control Objectives for Information and Related Technologies "COBIT 5 for Risk."

Now that we have an idea regarding some of the main security concepts and the notion of ROI as it pertains to the cyber security domain, we are ready to examine, in Chapter III, security control families from NIST SP 800–53 rev4, with an eye to which security principle(s) they may provide/promote, and what we might expect from them in terms of security ROI. Along with the need to discuss the system for which we select security controls, we must also discuss the selection and prioritization methodologies.

III. CYBER SECURITY CONTROLS

The Federal Information Processing Standard Publication 199 defines security controls as “the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information” [34].

A. NIST SP 800–53: AN INTRODUCTION

The National Institute of Standards and Technology develops and promotes the standards for industry and federal agencies. In order to support the implementation of the FISMA, the NIST Information Technology Laboratory has developed a series of special publications regulating various aspects of this matter. NIST SP 800–53 rev4 is a consolidated information security framework that provides a comprehensive set of security controls, three types of security control baselines, and the methodology and guidance for selecting a baseline along with specific security controls [7]. All these tools, if implemented correctly, can fundamentally fortify information systems and provide the near real-time information needed for risk-management decisions. This publication was developed based on a holistic and consistent approach to risk management and cyber security.

To establish a common foundation for cyber and information security, the Information Technology Laboratory collaborates and consults with other federal entities, including the Office of the Director of National Intelligence, the DOD, and the Committee on National Security Systems, in addition to organizations in the private sector. Such cooperation ensures a comprehensive expert vetting and systematical review, helps to avoid duplication of effort, and increases the overall efficiency of national cyber and information security efforts. The SP 800–53 publication is not a compliance, “checklist-type,” standard like PCI DSS (The Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability and Accountability Act of 1996). Rather, it is guidance that provides a well-structured catalog of controls needed for achieving compliance with most federal information assurance and cyber security standards. Also, this publication does not cover assessment of the correctness of security control implementation. Guidelines for performing such “correctness” are represented in a separate publication, NIST SP 800–53A “Guide for Assessing the Security Controls in Federal Information Systems and Organizations.”

B. THE SECURITY CONTROL FAMILIES

NIST SP 800–53 rev4 organizes all security controls into 18 distinct families based on the general security topic common for controls. All security controls focus on the fundamental security approaches and countermeasures. This publication mostly contains technology-neutral and policy-neutral controls. In other words, they are not tailored to any specific environment or technology. The tailoring process for application-specific matters is described in Chapter III of the publication.

As described in NIST SP 800–53 rev4, adherence to technology- and policy-neutral security controls has the following advantages, which encourage organizations to:

- Focus efforts on the *security capabilities* needed for mission success and the protection of information, irrespective of the information technologies used.
- Analyze each security control for its applicability to specific technologies, operational environments, and mission’s objectives.
- Specify security policies as part of the tailoring process for security controls that have variable parameters. [7]

The Table 1 presents security control families along with a brief description of each family’s content.

Table 1. NIST 800–53 rev4 Security Control Families

Identifier	**Security control family**	**Controls in the family**	**Brief description of the family content**
AC	Access Control	25	Contains access control policy and procedures Limits access to information and systems Provides guidance on defining roles and privileged accounts
AU	Audit and Accountability	16	Provides a mechanism to record incidents and security policy violations Provides guidance for log-collection Defines audit review, analysis, protection and reporting

Identifier	Security control family	Controls in the family	Brief description of the family content
AT	Awareness and Training	5	Defines security awareness and training policy and procedures Describes security awareness program, role-based training
CM	Configuration Management	11	Outlines configuration management policy and procedures Defines system baseline configuration and change restrictions Describes configuration management plan
CP	Contingency Planning	13	Focuses on contingency planning, training and testing Provides controls for system recovery and backup procedures, alternate security mechanisms
IA	Identification and Authentication	11	Describes identification and authentication (I&A) policies and procedures. Defines I&A Procedures for different types of users Details cryptographic aspects of identification and authentication
IR	Incident Response	10	Outlines incident policies and procedures Describes incident response planning, training, testing Describes incident monitoring, reporting, handling, and analysis
MA	Maintenance	6	Outlines system maintenance policy and procedures Describes maintenance tools, personnel aspects
MP	Media Protection	8	Outlines media protection policy and procedures Describes media access, marking, storage, transport, sanitization, use, downgrading
PS	Personnel Security	8	Outlines personnel security policy and procedures Details personnel screening, termination, transfer, sanctions
PE	Physical and Environmental Protection	20	Outlines physical and environmental policy and procedures Describes physical access control, authorization, monitoring Details support system policies and emergency procedures
PL	Planning	9	Outlines security planning policy and procedures Describes system security plan development, update Outlines rules of behavior, security architecture, central management
PM	Program Management	16	Identifies information security resources, inventory, workforce Outlines risk management strategy, enterprise architecture, critical infrastructure plan
RA	Risk Assessment	6	Outlines risk assessment policy and procedures Identifies security categorization Describes vulnerability scanning and monitoring
CA	Security Assessment and Authorization	9	Outlines security assessment and authorization policy and procedures Describes security certification and assessment Describes penetration testing
SC	System and Communications	44	Outlines system and communication protection policy and procedures

Identifier	Security control family	Controls in the family	Brief description of the family content
	Protection		Details implementation of protected communication with systems Identifies various technical aspects of network protection mechanisms, boundary protection Describes limiting direct hardware access
SI	System and Information Integrity	17	Outlines system and information integrity policy and procedures Describes malware protection, monitoring, and handling Identifies information input and output restrictions
SA	System and Services Acquisition	22	Outlines system and services acquisition policy and procedures Describes system development life cycle Defines software development, usage control, and documentation

NIST SP 800–53 rev4 divides all security controls into three categories: common controls, custom controls, and hybrid controls. Common controls are intended to be used throughout an agency for all of its information systems. Custom controls are suited to a particular system, or even for an individual device. Hybrid controls have characteristics of the previous two categories, and thus such controls are based on common controls but have been tailored for a particular system or component [7].

Many security controls have control enhancements aimed at increasing the effectiveness and strength of the main control. Control enhancements should be implemented in conjunction with the main control. Each family starts with the so-called "dash-1control," which defines policies and procedures required for implementation of the various controls included in the family. Many security controls have supplemental guidance intended to help define and implement a given security control by providing supplemental information. Supplemental guidance does not include any additional requirements to the control.

C. ENVIRONMENTAL SPECIFICS

This thesis is aimed at determining the top 10–20 security controls that would address security gaps of some information systems in order to achieve an acceptable level of risk. The information systems (IS) addressed here are those of computer networks deployed by military units on their permanent base facilities. The overall purpose of these

ISs is considered to be in support of process and exchange of various work-related documents and emails, Internet access, and the facilitation of infrastructure for several specific administrative applications. It is assumed that these ISs have been designed and built from the usability perspective, rather than with significant consideration for security. We assume the ISs' network architectures are based on the domain service management model, with a single Microsoft Active Directory Domain Controller that has the following characteristics:

- No group security policies are implemented.
- No network defense mechanisms are implemented, except regularly updated antimalware applications installed on workstations and servers.
- No security policy enforcement mechanisms are implemented.
- No workstation centralized management is implemented.
- No user activity monitoring and audit procedures are implemented.

From the other side, some security aspects are well handled due to strict military organizational policies and procedures. The following aspects are well enforced and audited (i.e., no additional security controls required):

- Physical security matters (e.g., physical access to network assets, video surveillance, guards).
- Personnel security matters (e.g., personnel screening, delegation of authorities).
- Environmental and life support system matters (e.g., electricity, cooling and heating, natural disaster).
- System and service acquisition (e.g., procurement security, vendor certification and screening).

To address the network vulnerability to basic types of attacks that can jeopardize a unit's mission, cyber capabilities should be developed in a short period of time (we suggest within six months) so as to facilitate a relatively rapid build-up of the "first line of defense." Environmental specifics render many potential security controls less necessary, or less effective than they would otherwise be. The suggested development time of only six months implies that any security controls that are very time consuming to implement, or that require extensive personnel training, will be deemed unacceptable to the goals of this research. Further filtering is applied for those security controls that are very costly in terms of initial investment, maintenance, support licensing, etc.

Therefore, the security controls for rapid cyber security development in resource constrained conditions would be mostly, but not necessarily limited to, fundamental *preventive* security controls that provide some immediate increase in cyber protective capability for the given network. According to a Center for Strategic and International Studies report, “more than 90% of successful breaches required only the most basic techniques” and “ 96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls” [53]. A good example of a security control with a very high ROI ratio would be that of deploying a password requirement policy that enforces complexity, non-reusability, and change period requirements. Implementation of this particular security control would, in most cases, not require deployment of high-end equipment, nor entail long and costly technical personnel training, nor the purchasing of licenses or other kinds of capital resource investments. However, this simple security control addresses a tremendous amount of cyber exploitation techniques and attack vectors. The result is a single security control (secure password management) that would yield high returns (‘R’) on security, for a relatively low investment (‘I’) of time, money, and personnel resources; i.e., a high ROI solution.

D. INDUSTRY RECOMMENDED STANDARDS

There are several top-lists of security controls that contain the most effective security controls prioritized by highest return. However, these “top-lists” predominantly do not consider the investments needed and resource constraints. The desire for rapid development of cyber security capabilities in a resource-constrained environment requires the selection of security controls with high ROI. We might refer to this approach to security control selection as the “quick win” approach. Industry recommended top security control lists do not take this ROI issue into consideration; instead, they focus completely, or at least predominantly, on the *Return* (‘R’) numerator.

The *Return* of candidate security controls was assessed based on the various cyber security reports, a series of SANS publications "What works case studies," and other materials on success cases. To analyze potential security controls from an *investment* perspective, we used the consistent, industry-standard approach to conduct assessment of costs: the "Total cost of ownership" (TCO) approach. Gartner defines TCO as "a comprehensive assessment of information technology or other costs across enterprise boundaries over time" [54]. To tailor TCO to cyber security technologies, we have considered the *initial* investments and the cost of ongoing *maintenance*. The initial investment in our analysis is presented by the following relative aspects:

1. cost of equipment or software required to implement a security control;
2. time needed for implementing a security control (in terms of time for deploy of equipment or software, configuring);
3. time required for training of technical personnel to obtain skills and knowledge needed for implementing the security control; and
4. potential user resistance caused by restrictions introduced by a security control.

Investment in maintenance considers the cost of purchasing annual licenses or other investments necessary to operate a security control. Due to various licensing policies and support models, maintenance costs can vary significantly, but should never be underestimated. According to the Gartner research on this matter, "80% of total IT costs occur after the initial purchase" [55]. Also, maintenance costs should take into account staff involvement in the ongoing operation of the security control. This involvement includes, but is not limited to, periodic audit activities, configuration updating and revision control, policy development, and security control review (e.g., certification and accreditation).

The following industry publications and recommendations on security controls were analyzed using the aforementioned perspectives:

"The CIS Critical Security Controls for Effective Cyber Defense" version 6 developed by the SANS Center for Internet Security (CIS). Published in October 2015. This document provides a comprehensive list of actionable guidance to mitigate the most pervasive and dangerous attacks. The list of controls was developed with a focus on the most common threats and attack patterns based on the leading cyber threat reports of government agencies and the private sector [56].

“Strategies to Mitigate Targeted Cyber Intrusions” developed by the Australian government’s Cyber Security Operations Center (ASCS), also known as the “Australian top 35.” Updated in February 2014. This publication contains an ordered list of 35 security controls and provides additional information on relative implementation costs and user acceptance levels [57].

“10 Steps to Cyber Security” developed by the United Kingdom National Cyber Security Center (UK NCSC). Updated in August 2016. This guidance provides high-level abstraction strategies on gradually achieving cyber security based on the risk management regime [58].

“10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks” developed by Water Information Sharing and Analysis Center Security Information Center (Water-ISAC) in partnership with the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the Federal Bureau of Investigation (FBI). Updated in June 2015. This document provides a list of ten fundamental cyber security recommendations for critical infrastructure systems in order to reduce system vulnerabilities and increase robustness against cyber threats [59].

“IAD’s Top 10 Information Mitigation Assurance Strategies” developed by the Information Assurance Directorate of the National Security Agency (NSA IAD). Published in December 2015. This publication, based on the “Brake the attack life cycle” approach, provides ten proactive mitigation security controls making networks defensible [60].

To develop a list of the top 10–20 security controls that address the “quick win,” high ROI, requirements of this study, and to do so in a methodical way, the analysis of the previously identified industry recommended controls and strategies was conducted according to the following steps:

1. Gather all recommended security controls from the aforementioned publications.
2. Eliminate of duplicates from the gathered list.
3. Eliminate security controls deemed to have such a high level of abstraction (i.e., “Implement network segmentation”) as too difficult to actually assess from an ROI perspective.
4. Eliminate costly and time-consuming security controls (i.e., those with a large “I” in the ROI calculus).
5. Select and prioritize security controls based on their qualitative ROI (priority to controls with lower investments).

This chapter has outlined the goals of the choice of top security controls. It presents the environmental specifics of the information system to secure, which in general can be described as “properly functioning network with no security cyber security implemented.” Also the chapter has presented the selection and prioritization approaches along with a short discussion of existing “top-lists” of recommended security controls. The next chapter enumerates the top security controls chosen, along with the “R” and “I” analysis that led to each being included in the top list.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SELECTION OF THE TOP SECURITY CONTROLS

This chapter presents the 13 security controls that this research believes provide the highest security ROI for any country or large enterprise that is trying to make quick and significant improvements to their cyber security posture. Each control has a general description of the security control or its underlying technologies. Each control is also provided with a qualitative estimate of its TCO. This TCO estimate includes; initial investments, time needed for the implementation, resources required to maintain the security control, potential user resistance, and required training. Moreover, the chapter provides a subjective analysis of the potential risk reduction, as a result of implementing the security control. Finally, the chapter provides some basic guidance and recommendations regarding each control's implementation.

A. RESTRICT USE OF ADMINISTRATIVE PRIVILEGES BY IMPLEMENTING GROUP SECURITY POLICY

This is a *Prevention* security control.

1. Description

An administrator account is the most powerful account in the Windows environment. Such power is not necessary for most users to perform their duties. According to the POLP, this account should be restricted to authorized personnel for very specific needs and should not be used on a daily/routine basis. Privileged accounts should be used for only for initial system configuration, troubleshooting, maintenance operations, conducting local audit, and other such rare operations.

Most exploitation techniques provide an attacker access to the privileges of the attacked account. So, if a user with administrative rights inadvertently launches malware, the malware will execute with the same administrative privileges as those of a system administrator. With such access, the malware can greatly harm the compromised system, and perform additional lateral movement attacks across the network. Besides that, non-malicious users with admin privileges could create vulnerabilities in the system as they have the ability to modify the system configuration, and install or delete software.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **5th** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **4th** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **2nd** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **4th** position in the "10 Steps to Cyber Security" (UK NCSC).
- **4th** position in the "10 Basic Cyber security Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

A security report by Avecto states that the most critical Microsoft vulnerabilities can be neutralized by removing admin rights: "removing admin rights would mitigate 98% of critical vulnerabilities affecting Windows operating systems, 95% of critical vulnerabilities affecting Microsoft Office and 99.5% of vulnerabilities in Internet Explorer" [61]. This security control has the potential to greatly constrain exploitation effectiveness. Moreover, according to [62], it makes the operating environment more stable, as well as easier to administer and troubleshoot, and less likely that a user may make inadvertent changes to his/her system that might introduce additional vulnerabilities.

c. Investment

- Initial investments—requires *no* additional equipment or software purchasing.
- Implementation time—*short* (up to two weeks). Depends on the size of the unit (number of users).

- Maintenance—does not require paid subscriptions or licenses. Does not require significant staff involvement.

- User resistance—while implementing the control the unit, technical personnel might encounter *medium* user resistance because of losing the ability to install software and configure the environment.

- Personnel training—may require short training time (two weeks) on the *Active Directory Group Policy configuration* for technical personnel implementing the security control.

3. Recommendations

This security control can be implemented using Windows Group Policy (WGP). It is the mechanism that can distribute privilege settings to all workstations where the administrative privileges need to be restricted. WGP also provides settings for tracking the usage of privileged accounts.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- AC—2 “Account Management” and

- AC—6 “Least privilege.”

B. ENFORCE STRONG PASSWORD POLICY (USER ACCOUNTS AND EMAILS) BY IMPLEMENTING GROUP SECURITY POLICY

This is a *Prevention* security control.

1. Description

A password is typically a secret string of characters that a claimant uses to authenticate its identity, as stated in [63]. Passwords are used to protect access to information, operating systems, hardware, and applications. A password is, in effect, a “key to the fortress.” A weak password is a portal for many exploitation techniques and can significantly decrease or even bring to naught other security controls and defense efforts.

The longer a user uses the same password, the greater the risk that an attacker might discover the password using brute force attacks. Moreover, Microsoft indicates that compromised accounts remain exploitable until the next password change [64]. Therefore, enforcement of this security control should consider the following aspects:

- restricting reuse of passwords (password history);
- setting maximum password age;
- setting minimum password length; and
- ensuring passwords meet complexity requirements.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **3rd** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **25th** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **7th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **2nd** position in the "10 Steps to Cyber Security" (UK NCSC).
- **5th** position in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

If a password complexity policy is not enforced, users will likely resort to selecting low-entropy passwords that are short and easy to remember. Such simple passwords are very easy to crack using automated dictionary or brute force attacks. Research by CynoSure Prime on 11.7 million cracked passwords shows that about 80% of them were not compliant with most industry recommendations and standards pertaining to password selection [65]. The research also shows that 78.6% did not match complexity requirements (e.g., contained only lower case letters) and 68.4% were too short (e.g., fewer than eight characters) [65]. Another study by TeleSign shows that 47% of users use a password that is at least five years old [66]. Strong passwords can mitigate password cracking and guessing attacks, and reduce the risk of compromise of applications using password-based authentication.

c. Investment

- Initial investments—requires *no* additional equipment or software purchasing.
- Implementation time—*very short* (two days).
- Maintenance—does not require paid subscriptions or licenses. Does not require significant staff involvement.
- User resistance—while implementing the control, the unit technical personnel might encounter *medium* user resistance due to usability disadvantages related to complex passwords.
- Personnel training—requires *no* additional training for technical personnel implementing the security control.

3. Recommendations

This security control for operating system accounts can be implemented using WGP. Enforcement of password policy for email accounts might be implemented through the configuring of the email server or application.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include IA–5 “Authenticator Management.”

Related publications and resources include:

- NISP SP 800–118 “Guide to Enterprise Password Management (Draft)” and
- Microsoft TechNet publication “How to Configure Security Policy Settings.”

C. ESTABLISH BASIC BOUNDARY DEFENSE BY DEPLOYING NETWORK INTRUSION PREVENTION SYSTEM

This is a *Preventive* and *Detection* security control.

1. Description

The network intrusion detection/prevention system is an enterprise security technology that identifies suspicious network events, then logs them, blocks them, and—optionally—sends a notification to a security administrator, as defined in [33]. It works by analyzing inbound and outbound network traffic using deep packet inspection. Unlike many firewalls, which only analyze packet headers and filter traffic based solely on protocol, network addresses and ports; an intrusion prevention system (IPS) analyzes a packet's headers and payloads, looking for indicators of real or potential malicious activity. That is why, topologically, an IPS is usually deployed after a network firewall. In such a scheme the firewall performs an important role of pre-filtering traffic before the IPS, which might otherwise be overwhelmed by a high volume of extra traffic.

One of the advantages of an IPS is that deployment of it usually does not require drastically changing existing network architecture. IPS deployment in the network topology is sometimes referred to as "bump in the wire." This implies that the IPS can be "inserted" on the network path ("wire") without having to make any configuration updates/changes to any other devices in the protected network. Another benefit of most modern IPSs is that they can perform threat prevention without extensive initial configuration. This is made possible by simply employing some or all of the many filter signatures that are made available by the vendor. Of further benefit is the fact that the update of these signatures are typically included as part of the licensing of the product. Further tailoring and creation of *custom* rules can further the effectiveness of an IPS, and decrease the occurrence of false-positives and false-negatives. However, such customized tuning requires some depth of technical understanding, by the rule developer, of the application and services used, normal network behavior, and other environmental specifics.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **12th** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **33rd** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **10th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **3rd** position in the "10 Steps to Cyber Security" (UK NCSC).
- **2nd** position in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

According to the Symantec study, "IPS protects against a wide range of security issues, which includes vulnerabilities, zero day exploits, exploit kits (EK), social networking threats, command and control (C&C) activities (back doors and botnets), online scams, malvertising, phishing, and many more" [67]. Furthermore, IPSs can also:

- identify reconnaissance activity, detecting scans, and probes;
- provide incident log information for incident investigation;
- identify potential violations of an organization's security policies;
- block specified application traffic; and
- prevent data exfiltration and monitor file transfers.

The IPS provides an additional layer of network defense and can potentially detect and block malicious activities that lesser-capable firewalls may not detect. According to the latest exhaustive tests of IPS solutions, security effectiveness ranged from 24.9% to 99.9% [68]. These tests covered the eight most popular, as of 2016, network IPSs, and included 1,986 exploits and 120 evasion techniques. In this research, the security effectiveness was based on a comprehensive score that included both exploit detection rates, and resistance to known evasion techniques. Along with this, a network-based intrusion prevention system (NIPS) can be used to troubleshoot network problems or measure and document typical network traffic and patterns; which can be valuable for statistics-based anomaly detection analysis.

c. Investment

- Initial investments—requires purchasing and deployment of several NIPS devices.
- Implementation time—*medium* (up to four weeks).
- Maintenance—requires paid subscriptions or licenses. Requires *medium* 24/7 staff involvement for monitoring security events and NIDS reports.
- User resistance—while implementing the control, technical personnel likely encounter *low* user resistance, as it does not affect user experience and usability.
- Personnel training—may require a vendor-specific short-time training (two weeks) on the *NIPS deployment, initial configuration, and tuning* for technical personnel implementing the security control.

3. Recommendations

The IPS can be implemented as software or hardware. Typically IPS infrastructure consists of network sensors, an administrator console with a graphical user interface, and possibly an analysis and database server. Placement of an IPS mostly depends on network architecture, services provided, and available sensors. However, it is prudent to place it behind a screening firewall that is denying all traffic that is not essential to business or operations. Doing so should reduce the workload of the IPS and reduce the possibility of it becoming a network bottleneck. To detect, localize, and prevent propagation of attacks inside of the network, the IPS should be placed on the network segments' borders (i.e., entry-/exit-points).

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- SI–4 "Information System Monitoring" and
- SC–7 "Boundary protection."

Related publication—NIST SP 800–94 "Guide to Intrusion Detection and Prevention Systems (IDPS)."

D. DEVELOP BASIC RECOVERY CAPABILITY BY PERFORMING REGULAR BACKUP OF SERVERS

This is a *Recovery* security control.

1. Description

From a CIA-triad perspective, backups can help to maintain availability of data. In many areas, and specifically in military operations, data is the most valuable asset of a computer system. Unlike, for instance, an operating system that can be easily (relatively) reimaged or reinstalled, mission crucial data, if not backed up, are very difficult to recreate. Back up, in general terms, means to create copies of information and store it in a secure location that is sufficiently separated/isolated from the original data source. The degree of separation/isolation, and the complexity of the duplication (e.g., RAID, remote site, journaled, full- vs. differential-backup, etc.) can be determined by rather simple impact analysis. Such analysis would consider the potential harm to the organization's mission or business should certain data be lost. The investment made in the back up capability should then be in direct proportion to the determined potential harm. This is a straight-forward application of risk management.

It is essential to have backups of important information, as such data can be physically destroyed, logically destroy data (e.g., deleted), encrypted by ransomware, or lost due to some natural disaster; among other possibilities. For instance, Backblaze's research shows that 22% of hard drives experience a hard crash in the first four years of utilization [69]. Another study claims that "hardware or system failure accounts for 78% of all data loss" [70]. After such incidents, whether intentional or accidental, it is relatively easy to restore information from backups, if such backups are available. Having such backups readily available would significantly reduce the harm caused by any incident that involved the destruction of data.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **10th** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **Not included** in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **Not included** in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **Not included** in the "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

Return on this security control can be expressed in terms of potential harm mitigated by data recovery. For example, according to business statistics, "93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately" [71]. In the military sphere, the ability to restore corrupted data in a timely manner can be a key factor for mission success. Even organizationally and technically simple methods of full disk imaging backup can mitigate dozens of devastating scenarios when crucial data are lost. This simple approach has very low upfront cost due to cheap storage memory, but has very high return in terms of fast restoration of valuable data lost.

c. Investment

- Initial investments—requires purchasing and deployment of network data storage.
- Implementation time—*very short* (two days).
- Maintenance—does not require paid subscriptions or licenses. Requires *low* staff involvement.

- User resistance—while implementing the control, technical personnel will likely encounter *low* user resistance, as it does not affect user experience and usability.
- *No* additional training is required for technical personnel implementing the security control.

3. Recommendations

At minimum, primary servers providing core services should be backed up at least once per week. As a starting technique, external low-cost storage can be used to store copies of servers' hard drives. Various open-source software or software provided with hardware solutions can be used to automate this process. The following recommendations of the Massachusetts Institute of Technology should be considered for backup enhancement.

- Encrypt backups that contain sensitive data.
- Keep extra backups off-site in a secure location (in case of property damage).
- Verify your backups to make sure files are retrievable.
- Sanitize or destroy your backups (e.g., tapes, CDs) before discarding them. [72]

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- CP–9 "Information System Backup" and
- CP–10 "Information System Recovery and Reconstitution."

Related publication and resources include:

- NIST SP 800–34 rev1 "Contingency Planning Guide for Federal Information Systems" and
- Microsoft TechNet publication "Backing Up Your Server."

E. MITIGATE GENERIC EXPLOIT TECHNIQUES BY DEPLOYING ENHANCED MITIGATION EXPERIENCE TOOLKIT

This is a *Prevention* and *Detection* security control.

1. Description

Many operating systems provide anti-exploitation features that monitor running applications for common exploitation techniques. In the Windows environment, the most used tool set for the operating system (OS) generic exploit mitigation is the Enhanced Mitigation Experience Toolkit (EMET). According to the "IAD's Top 10 Information Mitigation Assurance Strategies," EMET can provide "fundamental protection against common classes of exploitation used as building blocks of zero day attacks" [60]. This free security tool, distributed by Microsoft, can make system flaws very hard to exploit. It focuses on breaking exploitation techniques by applying mitigation technologies (e.g., injecting an EMET.dll into running executables) to applications. When EMET detects an attempt to exploit running application, it shuts down the attacked application and notifies the user. EMET is not application specific, and works even with legacy software. Functionally, the EMET provides vulnerability mitigation after the firewall and before antimalware application. Security tools like Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), included in the EMET, significantly reduce the attack surface of an operating system and the individual applications running on it. EMET is constantly evolving and has more security tools included. Additionally, EMET can identify the processes that are not using DEP, and can then enable it on the process' underlying application, without having to recompile the application.

ASLR can prevent many exploitation techniques by randomizing the location of data in memory. ASLR makes the layout of applications' address space different on all workstations. As a result, an attacker cannot make logical assumptions about a targeted object's (i.e., code) location in memory. DEP prevents exploitation techniques based on a direct injection and execution forged programming code from locations of memory intended for data.

2. Justification

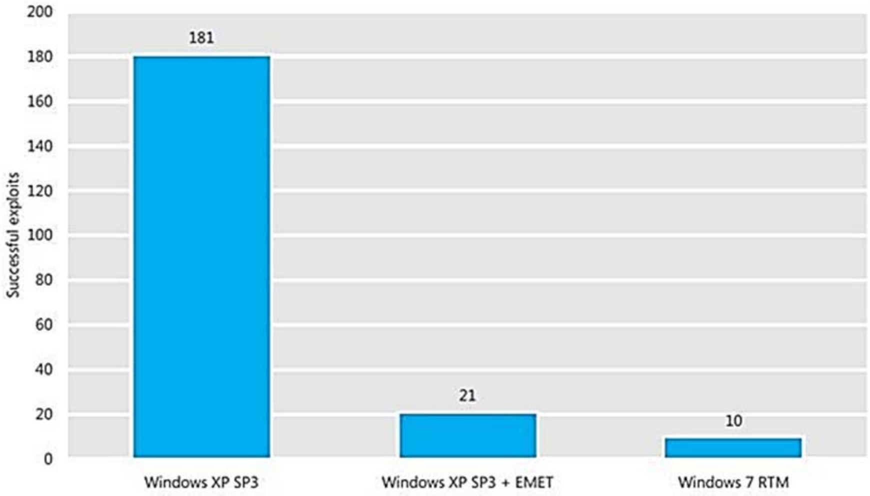
This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **8th** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **7th** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **5th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **7th** position in the "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

Generic exploit mitigation tools can provide an additional layer of defense against common exploitation techniques and malware attacks. According to the latest Microsoft research on EMET effectiveness against the most popular application used with Windows operating systems, EMET drastically reduces the exploits' effectiveness on Windows XP. From 184 application exploits collected from the company's customers worldwide, only 21 exploits succeeded on Windows XP protected by EMET [73]. Figure 3 shows the results of the study.



The Risk Management Framework provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Source: Microsoft's Free Security Tools – Enhanced Mitigation Experience Toolkit.

Figure 3. The Effectiveness of 184 Exploits for Popular Applications on Windows XP, Windows XP with EMET Deployed, and Windows 7. Source: [73].

c. Investment

- *No* additional equipment or software purchasing is required.
- Implementation time—*short* (up to one week).
- Maintenance—does not require paid subscriptions or licenses. Does not require significant staff involvement.
- User resistance—while implementing the control, technical personnel will likely encounter *low* user resistance, as it does not affect user experience and usability.
- *No* additional training is required for technical personnel implementing the security control.

3. Recommendations

EMET starting with version 3.0 has integrated functionality for enterprise deployment and centralized configuration. The deployment can be performed through the use of Group Policy or System Center Configuration Manager (SCCM). These technologies also enable large-scale enterprise configuration and monitoring.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include SI–3 “Malicious code protection.”

Related publication include the “Enhanced Mitigation Experience Toolkit (EMET) 5.52 User Guide.”

F. ENHANCE END-POINT SECURITY BY DEPLOYING HOST INTRUSION PREVENTION SOLUTION

This control is *Prevention* and *Detection* security control.

1. Description

A host intrusion prevention system (HIPS) is often used as an additional layer of protection for an individual device: workstation or server. HIPS can be integrated with an antimalware solution, or can be deployed as a separate dedicated solution. In contrast with antimalware software, which works by comparing machine code to the known malicious code patterns (signatures), HIPS can stop malware and other malicious activities by monitoring the *behavior* of the running processes. In this way, HIPS can provide a certain level of protection against unknown “zero day” threats, as a HIPS does not depend on specific threat signatures.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended “Top-lists”

- **8th** position in the “The CIS Critical Security Controls for Effective Cyber Defense” (SANS CIS).
- **8th** position in the “Strategies to Mitigate Targeted Cyber Intrusions” (ASCS).
- **6th** position in the “IAD’s Top 10 Information Mitigation Assurance Strategies” (NSA IAD).
- **7th** position in the “10 Steps to Cyber Security” (UK NCSC).

- **4th** position in the “10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks” (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

HIPS can substantially enhance protection of the end-user workstations and servers by adding an additional layer of defense to signature-based antimalware. The HIPS can mitigate various host-aimed threats and intrusion activities typically undetectable by traditional antimalware. One of the biggest benefits of HIPS, is that unlike NIPS, it can be customized to an individual system. Such customization can take into account the specifics of the workstations or servers with respect to the applications installed, services provided, user roles, etc. This, in turn, can decrease the rate of false positive alerts. Most HIPS also provide defenders with the means to create custom rules that can help to localize and eradicate recently discovered threats and exploits. HIPS can be an effective tool for the detection of APT activities in the network based on the hosts’ alerts. Along with this, HIPS can detect attacks that use encrypted traffic; whereas a NIPS solution could not.

c. Investment

- Initial investments—requires purchasing software. Some solutions may require deploying a dedicated update server.
- Implementation time—*medium* (up to four weeks).
- Maintenance—requires paid subscriptions or licenses. Does not require significant staff involvement.
- User resistance—while implementing the control, technical personnel will likely encounter *low* user resistance, as it does not affect user experience and usability.
- Personnel training—requires *no* additional training for technical personnel implementing the security control.

3. Recommendations

To reduce the TCO, the HIPS should be integrated with the antimalware solution where the environment allows it. Using an integrated solution (HIPS + antimalware) instead of two separate solutions will decrease investments needed for purchasing end-point security solutions. It also reduces the involvement of staff in terms of the security controls deployment, configuration, and monitoring. A HIPS integrated with antimalware software or end-point protection suites provides basic functionality, but is relatively easy to deploy.

In the case where a separate, non-integrated, HIPS solution is used, it can be remotely deployed using the WGP. Dedicated HIPS solutions usually provide more advanced functionality and better protection. However, we do not recommend using them for rapid cyber capability development. Because dedicated HIPS in most cases will require higher investments. Along with this, they might require significant effort, knowledge, and skills for tailoring and further tuning. Also, some dedicated HIPS might not be compatible with antimalware installed on the host.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- SI–4 "Information System Monitoring" and
- SI–3 "Malicious code protection."

Related publications include NIST SP 800–94 "Guide to Intrusion Detection and Prevention Systems (IDPS)."

G. CONTROL SOFTWARE EXECUTION BY IMPLEMENTING APPLICATION WHITELISTING

This is a *Prevention* security control.

1. Description

NIST defines an application whitelist as "a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline" [74]. Software whitelisting is a proactive security technique that allows users to run only approved software and prevents execution and installation of all other applications on the system. Software whitelisting technologies and control programs are intended to prevent the execution of malicious code or any other unauthorized applications. Unlike antimalware programs, which implement blacklisting (i.e., block known harmful operations and permit any other), software whitelisting helps to reduce the target surface area by not even allowing the possibility of code to run, when that code is associated with applications deemed non-essential to an organization's mission.

A whitelist should include software necessary for the user to perform assigned duties. Each application increases the system's attack surface by introducing potential security flaws. Therefore, the whitelist should be as narrow as possible and carefully developed in adherence with the POLP. This security control is a very effective tool for blocking malware execution. However, some infection techniques can evade whitelisting by malicious memory injections, interpreted code, Java shell code or macros, and kernel-level attacks. Nevertheless, as stated in [75], software control, in most cases, can prevent morphing of the initial compromise into a situation in which the malware or attacker obtains full control.

Computers without software whitelisting mechanisms implemented are more likely to be infected by malware and to violate copyright laws, by running software that is unnecessary to mission tasking. Attackers often use infected computers as a staging point for further propagation into the network. This includes, but is not limited to, collecting sensitive data from exploited workstations, servers, and network devices, and launching attacks against other systems connected to compromised ones. This, according to SANS, can lead to turning one compromised computer into many [56].

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **2nd** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).

- **1st** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **1st** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **7th** position "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

In the Gartner report on protection of endpoints by application control, application control is described as "a very effective method to block malware-based attacks, including new and targeted attacks, malicious insider attacks and dangerous user behavior" [75]. According to the report, control of whitelisting software execution has the following advantages:

- Reduces the frequency and severity of malware incidents.
- Detects potential insider threats or user policy violation attempts (for instance, downloading hacking tools, attempts to load unauthorized applications).
- Blocks unwanted potential backdoor applications not detectable by antimalware.
- Reduces vulnerabilities by limiting software sprawl (that is, multiple browsers and related plug-ins, Adobe/browsers on servers).
- Blocks common malware techniques and indicators of compromise (for instance, no execute from trash bin, no double extensions, and no header extension mismatches).
- Provides incident response and investigation capabilities, such as a search of all workstations with certain executable files, removal of unwanted or malicious software already installed, and blocking newly discovered malware before corresponding blocking signatures become available. [75]

c. Investment

- Initial investments—*no* additional equipment or software purchasing required.

- Implementation time—*medium* (up to four weeks). Depends on variety of software used in the unit, variety of employee roles and needs, use of the uncommon applications.
- Maintenance—does not require paid subscriptions or licenses. Requires *medium* staff involvement.
- User resistance—while implementing the control, the unit technical personnel might encounter *medium* user resistance due to losing the ability to install software and run unspecified software.
- Personnel training—requires *no* additional training for technical personnel implementing the security control.

3. Recommendations

Software whitelisting can be implemented using MS Windows built-in tools (Software Restriction Policies and AppLocker), application execution tools that come with antimalware software or by implementing more expensive commercial whitelisting tools. Along with that, many of today's endpoint security suites, personal firewalls, and host intrusion detection systems provide features performing pre-launch checks of an application's name, location, hash, vendor's certificate, and other parameters to determine whether this software can be run. Windows' built-in tools provide basic application control capabilities. However, they do not provide the means for centralized monitoring and management of application execution.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- CM-8 "Information System Component Inventory,"
- CM-10 "Software Usage Restrictions," and
- CM-11 "User-installed Software."

Related publications and resources include:

- NIST SP 800–167 "Guide to Application Whitelisting" and
- NIST SP 1800–5 "IT Asset Management Practice Guide."

H. ESTABLISH SYSTEMATIC OPERATING SYSTEM PATCHING BY DEPLOYING UPDATE SERVER

This is a *Prevention* security control.

1. Description

A patch is the change introduced into a piece of programming in order to fix discovered security or functionality issues, or to add new functionality. NIST defines patch management as “the process for identifying, acquiring, installing, and verifying patches for products and systems” [76]. The intent of security patching is to correct security flaws in software and firmware and in this way to mitigate software vulnerabilities. Performing security patching in a systematic and timely manner (the higher vulnerability to be patched—the higher the priority) can significantly reduce the risk of exploitation. On the contrary, delays in implementing already released updates increase the risk of successful exploitation of the vulnerable software. After a security patch release, information about a discovered software vulnerability becomes publicly available. According to the Microsoft publications, many successful attacks using security flaws are performed a short time after such security update releases [77].

These updates are usually developed and released by software vendors for no additional cost to users. This release is typically conducted on a periodic basis. For instance, Microsoft releases patches for the Windows operating system every Tuesday. However, security updates for very critical vulnerabilities discovered might be done earlier than a typical schedule. According to SANS, “Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain” [78].

2. Justification

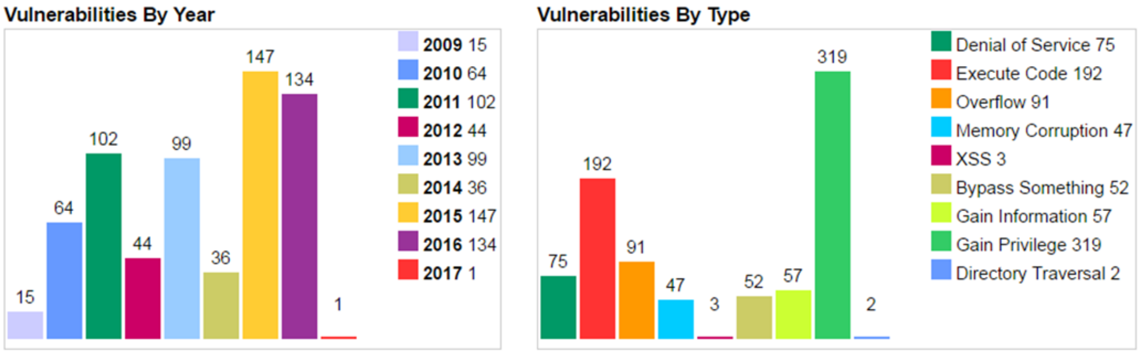
This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **4th** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **3rd** position in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **9th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **2nd** position in the "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

Implementation of this security control can significantly decrease the number of successful exploitations of systems and application vulnerabilities. According to the Center for Strategic and International Studies report, 75% of attacks could be prevented by regularly deploying patches [53]. The Common Vulnerabilities and Exposures database, which contains information on publicly known vulnerabilities, demonstrates that operating systems can have many vulnerabilities. For instance, the Windows 7 operating system which, despite being designed with serious consideration of security, still has hundreds of vulnerabilities of various types discovered every year (Figure 4). Most, if not all, of these vulnerabilities can be fixed by timely patching; otherwise, they *will* be exploited by attackers. Some of these vulnerabilities can lead to high criticality incidents that can potentially jeopardize mission accomplishment.



Windows 7 operating system has numerous vulnerabilities that can be patched, otherwise exploited by attackers. Details: Microsoft Windows 7 Vulnerability Statistics.

Figure 4. Windows 7 Vulnerability Overview. Source: [79].

c. Investment

- Initial investments—requires purchasing and deployment of a dedicated update server with Windows Server operating system.
- Implementation time—*medium* (up to four weeks).
- Maintenance—does not require paid subscriptions or licenses. Does not require significant staff involvement.
- User resistance—while implementing the control, the technical personnel will probably encounter *low* user resistance, as it does not affect user experience and usability.
- Personnel training—requires a short-time training (two weeks) on the *Windows Server Update Service (WSUS) deployment and configuration* for technical personnel implementing the security control.

3. Recommendations

Patch management can be implemented with Microsoft features (i.e., WSUS) and free services (i.e., Windows Update) well integrated with Microsoft Active Directory architecture. Third-party software provides additional features and functionality. However, it requires higher initial investments and paid annual licenses.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include SI–2 "Flaw Remediation."

Related publications and resources include:

- NIST SP 800–40 rev3 “Guide to Enterprise Patch Management Technologies” and
- Microsoft TechNet publication “Windows Server Update Services Overview.”

I. PERFORM USER ACTIVITY MONITORING AND SYSTEMATIC AUDIT BY IMPLEMENTING GROUP SECURITY POLICIES

This control is a *Deterrence* and *Detection* security control.

1. Description

User activity monitoring is the security practice of monitoring and recording actions executed by users on the computer system. Monitored activities can include access to sensitive information, file/object operations (creation/modification/deletion), logon/logoff events, use of applications, access to network resources and services, etc. User activity monitoring and audits should not cover all resources and activities as this could result in generating too much data, including myriad benign audit entries that offer little in the way of true-positive detection of malicious activity. This, in turn, could overwhelm an auditor and hinder his/her ability to identify truly malicious activities. Thus, monitoring and audit should include only the most critical events and objects. Special attention should be paid to privileged permissions used by administrator accounts, as such activities, if misused, can cause the most damage. The following administrative activities are good examples of what *should* be audited: security policy modification or cancelation, creation of new administrator or user accounts, changing access permissions for folders and files with sensitive information, failed logons to the administrator accounts, clearing of the audit logs, and stoppage of any security control.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended “Top-lists”

- **6th** position in the “The CIS Critical Security Controls for Effective Cyber Defense” (SANS CIS).
- **6th** position in the “Strategies to Mitigate Targeted Cyber Intrusions” (ASCS).
- **Not included** in the “IAD’s Top 10 Information Mitigation Assurance Strategies” (NSA IAD).
- **7th** position in the “10 Steps to Cyber Security” (UK NCSC).
- **4th** position in the “10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks” (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

Account monitoring and audit is a powerful tool to enhance the security of an organization. This security control supports accountability and acceptable use policy. For instance, if users are aware that they are being monitored, the risk of detection and corresponding punishment make policy violations or irresponsible behavior less likely. Thus, user activity audit and monitoring is a powerful factor for deterring users from violating security policies. In this way it can be a mitigation factor against an insider threat. And insiders, according to the Intel report, were responsible for 43% of data loss, and 50% of these accidents were intentional [80].

This security control can also be used for other various purposes, such us incident investigation, computer forensics, security policy compliance, and troubleshooting. Audits are also used for detection of suspicious behavior, to identify and mitigate flaws in security mechanisms implemented.

c. Investment

- Initial investments—*No* additional equipment or software purchasing required.
- Implementation time—*medium* (up to four weeks).

- Maintenance—does not require paid subscriptions or licenses. Requires *significant* staff involvement for continuous audit activities.
- User resistance—while implementing the control, technical personnel will likely encounter *low* user resistance as it does not affect user experience and usability.
- Personnel training—requires a short-time training (two weeks) on the *Advanced Security Audit policy settings* for technical personnel implementing the security control.

3. Recommendations

The Windows operating system provides a logging functionality to establish a tracking system that can record information about system and security events associated with potential violations and harmful behaviors. User activity monitoring and account audit can be implemented through the Advanced Security Audit policy settings. This WGP feature contains 53 different audit settings on audit events for specific activities and events. For planning purposes, it is necessary to identify the unit's most critical resources and the most important activities that need to be tracked. This typically includes the changes to security policies, changes to user accounts, use of administrative privileges, successful and unsuccessful logon events, modification of certain files and folders, etc.

For legal purposes, the informational disclaimer should be displayed after every logon. The disclaimer should contain a warning that user activities on this governmental system are being monitored according to the security policy.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- AC–2 "Account Management,"
- AC–3 "Access Enforcement,"
- AC–7 "Unsuccessful Logon Attempts," and
- SI–4 "Information System Monitoring."

Related publications and resources include:

- NIST SP 800–92 "Guide to Computer Security Log Management" and

- Microsoft TechNet publication "Audit data and user activity."

J. PREVENT UNAUTHORIZED DEVICES FROM GETTING NETWORK ACCESS BY DEPLOYING AAA-SERVER

This is a *Prevention* and *Detection* security control.

1. Description

Personal devices connected to an organization's operational network can result in access vectors for attackers, as personal devices often have unpatched software, out-of-date antimalware, and improper security settings that are easy to exploit. Thus, only authorized devices that are compliant with an organization's security policy should be permitted to connect to the network. Preventing access to the network by unauthorized devices is usually enforced through network access control or network admission control (NAC) solutions.

NAC typically includes the identification of the device, authorization and a check for compliance with security policy. However, this security control does not consider the last component, as a security compliance check requires the deployment of dedicated servers and configuring complex decision delegation schemes. Authentication and authorization components can by implemented by deploying an AAA server (authentication, authorization, and accounting) that handles user requests for access to network resources.

According to NIST SP 800–53 rev4, device identification is typically performed using MAC-address and IP-address authentication—by IEEE 802.1x and Kerberos protocols and remote authentication dial-in user service (RADIUS) server. The current *de facto* standard used for interaction between devices and an AAA server is RADIUS. This service is integrated on Windows Server operating systems as the Network Policy Server as a component of Network Policy and Access Services.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **1st** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **Not included** in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **10th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **3rd** position in the "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

NAC is a fundamental security control. Failure to perform NAC can potentially diminish the effectiveness of other security controls and protection mechanisms. It is a difficult task to protect the network when a vulnerable or infected device can be introduced to the network unseen. Moreover, providing uncontrolled network admission can result eventually in a malicious insider connecting a personal device loaded with tools to perform attacks from within a defensive perimeter. By implementing even a basic "go/no-go" solution, NAC can effectively limit the possibility of such cyber incidents from occurring.

SANS, in its white paper on NAC, highlights that the deployment of NAC allows IT-teams to "more readily track assets, see possible issues and address potential violations" [81]. Organizations that have implemented advanced NAC solutions, according to the research of ForeScout on the effectiveness of NAC, "experience 50% fewer network-related security breaches" [82]. Also the research indicates that deployment of NAC results in identifying 24% more of the devices on the organization's network.

c. Investment

- Initial investments—requires purchasing and deployment of a dedicated AAA server.
- Implementation time—*significant* (up to two months), requires reconfiguring all network access switches.
- Maintenance—does not require paid subscriptions or licenses. Requires *low* staff involvement.
- User resistance—while implementing the control, technical personnel will likely encounter *medium* user resistance as it constraints BYOD-approach.
- Personnel training—may require a vendor-specific short-time training (two weeks) on the *Configuring the RADIUS and TACACS+ protocols* for technical personnel implementing the security control.

3. Recommendations

This security control can be implemented by deploying various network access control technologies. For instance, Microsoft provides Network Access Protection platform and protocols. According to Chris Boscolo, one key benefit of NAP is that it can receive and process information from most antimalware applications via the Windows Security Center [83]. Cisco has the Network Admission Control Framework that provides numerous tools and protocols that can comprehensively mitigate threats related with unauthorized device connection issues. Cisco's NAC allows network access only to security policy compliant devices and restricts the access of noncompliant ones.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- IA–3 "Device Identification and Authentication" and
- CM–8 "Information System Component Inventory."

Related publications and resources include:

- Microsoft TechNet publication "Network Policy Server" and
- Cisco publication "Network Admission Control Framework Deployment Guide."

K. ENHANCE BOUNDARY DEFENSE BY CONFIGURING ACCESS LISTS ON THE BORDER AND INNER ROUTERS

This is a *Prevention* and *Detection* security control.

1. Description

Routers and switches, the devices that transport data across and between networks, are fundamental components of modern network topologies. These devices are also targets for numerous cyber attacks. However, properly configured routers can become the first layer of defense from external attack by performing basic traffic filtering. One of the main security features most routers and switches can implement is the access control lists (ACL) feature. Cisco defines ACL as a set of rules that specifies conditions that a packet must satisfy to match the rule [84].

An ACL can be applied to each of the routers' interfaces to filter both inbound and outbound traffic going through the interface. Most network equipment vendors provide two types of ACLs, standard and extended. Standard ACL provides a means to permit or deny traffic based on specific source address. Extended ACL provides more flexible filtering rules using both the source and destination address and the port number and protocol. The following list from Cisco provides some filtering options available in modern routers:

- Layer 4 protocol,
- TCP and UDP ports,
- ICMP types and codes,
- IGMP types,
- Precedence level,
- Differentiated Services Code Point (DSCP) value,
- TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set,
- Established TCP connections. [84]

Even though router ACLs provide rather basic traffic-based security filtering, they form an important first layer in the "defense in depth" approach. SANS explains this principle as applying many different security mechanisms instead of one. Thus, if one network defense layer is breached, an attacker still needs to overcome all other defense layers [85].

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **9th and 11th** positions in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **12th and 13th** positions in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **10th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **10th** position in the "10 Steps to Cyber Security" (UK NCSC).
- **2nd** position in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

Implementation of this control can protect the router itself from numerous threats and also can provide protection of inner network components placed behind the router. For instance, Cisco routers have ACLs that provide flexible options to mitigate a variety of cyber threats. This includes exploits that require specific network ports, DDoS attacks, and the basic mitigation of application-level attacks. Routers with configured ACLs face and reject unnecessary and unwanted traffic before other network security solutions. In this way ACLs can significantly decrease the number of security events generated by IDS and IPS solutions, thus decreasing the number of event logs recorded. Implementing ACLs does not require investments in purchasing equipment, as routers are already deployed. However, implementing ACLs require time and skills to develop filtering rules, configure them, verify their correctness and effectiveness. All in all, ACLs, configured on deployed routers, can provide defenders with the means to create another layer of defense by establishing network segmentation. Network segmentation is a security technique that divides a network into separate segments based on their trust level and functions in accordance with POLP. For example, for data leakage prevention purposes, ACLs can reject all Web traffic *from* a high-security network that is attempting to be routed *to* the Internet.

The ACL is also a key concept and main technique used in the deployment of firewalls; i.e., identify the metrics of particular traffic that should or should not be permitted to cross a given network interface, then craft an appropriate rule to filter such traffic accordingly. In the perspective of ROI-based selection of security controls, this control has a very low investment denominator as compared to more expensive and complex dedicated firewall appliances. Firewalls provide more advanced ACL-based protection, and they have better performance on filtering tasks than do routers that were not inherently designed for such additional tasking. However, configuring ACLs on routers and compatible switches does not require any upfront spending. Routers and switches form network and internetworks, so they are already a necessary and intregral part of an organization's IT infrastructure. This is in contrast to firewalls that require purchasing devices separately, as well as the added involvement of staff for their proper deployment.

c. Investment

- Initial investments—requires *no* additional equipment or software purchasing.
- Implementation time—*medium* (up to four weeks); requires reconfiguring all routers and compatible switches.
- Maintenance—does not require paid subscriptions or licenses. Requires *low* staff involvement.
- User resistance—while implementing the control, technical personnel will likely encounter *high* user resistance as it may significantly constraint users' access to entertainment Internet resources.

- Personnel training—may require a vendor-specific short-time training (two weeks) on the *Configuring the ACLs on routers and switches* for technical personnel implementing the security control.

3. Recommendations

Implementation of this security control requires careful preparation and listing of services required for the host organization's missions. Each service requires certain network ports and protocols to be allowed to pass from one network to the next. These specifics should be listed by technical personnel during the implementation, as this data is a necessary precondition for creating appropriate rulesets. There are two opposite basic strategies for rule creating: "whitelisting" (only permit what is necessary) and "blacklisting" (only deny what is known to be bad). Blacklisting may be not reliable as it is nearly impossible to create rules blocking all possible threats. A network port that is safe, and thus not blocked today, might be used tomorrow by a new type of malware. NIST SP 800–53 rev4 recommends implementing boundary protection with a strategy of "DENY BY DEFAULT / ALLOW BY EXCEPTION" [7]. Basically, if the content is not explicitly allowed by an ACL rule, the traffic will be rejected by the router. Such an approach is much easier to manage and implement than "blacklisting." With the "deny by default" approach, technical personnel have to manage only a small list of the specifically permitted rules. Furthermore, defenders do not have to constantly create new filtering rules to block recently discovered threats.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- SC–7 "Boundary Protection" and
- AC–4 "Information Flow Enforcement"

Related publications and resources include:

- NIST SP 800–41 "Guidelines on Firewalls and Firewall Policy,"
- NSA System and Network Attack Center publication "Router Security Configuration Guide," and
- Cisco publication "Protecting Your Core: Infrastructure Protection Access Control Lists."

L. IMPROVE INCIDENT RESPONSE CAPABILITY BY DEVELOPING INCIDENT HANDLING PROGRAM

This is a *Deterrence, Prevention, Detection,* and *Recovery control* security control.

1. Description

For virtually every network connected to the Internet, the occurrence of a cyber security incident is a matter of not “if,” but “when.” Incidents can have various levels of impact on the mission. UK NCSC recommends managing and analyzing all security incidents, especially “… those serious enough to warrant invoking the organization’s business continuity or disaster recovery plans. Some incidents can, on further analysis, be indicative of more severe underlying problems” [86]. According to the Information Technology Infrastructure Library, one of the best practices framework in the IT sphere, the two primary objectives of incident management are quickly recovering normal service and minimizing adverse impact [87]. UK NCSC in its guidelines on cyber security highlights that failure to manage incidents may lead to more severe impact, and a failure to address the root cause of a security incident can result in repetitive or even continuous compromise [86].

The heart of any cyber incident response capability is an incident handling program. A directive (CJCSM 6510.01B) on the “Cyber Incident Handling Program” from the *Chairman of the Joint Chiefs of Staff Manual* emphasizes that, “this program ensures an integrated capability to continually improve the Department of Defense’s ability to rapidly identify and respond to cyber incidents that adversely affect DOD information networks and information systems (ISs)” [88]. The incident handling program should be reflected in the set of policies, guidance, manuals, and technical instructions. This document should provide comprehensive information on handling processes and procedures. Development of the program should be based on the Manual’s recommended cyber incident handling process phases (cycle), which include:

1. Detection of events.
2. Preliminary analysis and identification of incidents.

3. Preliminary response actions.

4. Incident analysis.

5. Response and recovery.

6. Post-incident analysis. [88]

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **19st** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **Not included** in the "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **Not included** in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **6th** position in the "10 Steps to Cyber Security" (UK NCSC).
- **10th** position in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

The Information Technology Infrastructure Library lists the following major benefits of implementing an incident management process.

For the business as a whole, benefits include:

- reduced business impact of incidents by timely resolution, thereby increasing effectiveness;
- the proactive identification of beneficial system enhancements and amendments; and
- the availability of business-focused management information related to the service level agreement.

For the IT team in particular, benefits include:

- improved monitoring, allowing performance against service-level agreements to be accurately measured;
- improved management information on aspects of service quality;
- better staff utilization, leading to greater efficiency;
- elimination of lost or incorrect Incidents and service requests;
- more accurate configuration management database information (giving an ongoing audit while registering Incidents); and
- improved user and customer satisfaction. [89]

The Information Technology Infrastructure Library also highlights potential risks that can result from failing to establish incident management:

- no one to manage and escalate Incidents – hence Incidents may become more severe than necessary and adversely affect IT service quality;
- specialist support staff being subject to constant interruptions, making them less effective;
- business staff being disrupted as people ask their colleagues for advice;
- lack of coordinated management information; and
- lost, or incorrectly, or badly managed Incidents. [89]

c. Investment

- Initial investments—requires *no* additional equipment or software purchasing.
- Implementation time—*significant* (up to six months).
- Maintenance—does not require paid subscriptions or licenses. Requires *low* staff involvement.
- User resistance—while implementing the control, technical personnel will likely encounter *low* user resistance as it does not affect user experience and usability.
- Personnel training—may require a training (one to two months) on the *Development of cyber incident handling program* for management personnel implementing the security control.

3. Recommendations

In the framework of rapid cyber capability development, initial efforts should be focused on the development of incident triage procedures. After development, implementation and testing of the triage flow, escalation criteria, policies, plans, and procedures should be developed. Various publicly available incident management frameworks can be used as the basis for the development of an incident handling program. We suggest using the recommendation of NIST SP 800–61 rev2 “Computer Security Incident Handling Guide.” The guide provides a comprehensive and systematic approach in this matter, and—as an added benefit—is integrated with other NIST special publications (SPs) that are recommended by this report (e.g., SP 800–53).

The structure of primary documents of an incident handling program, as recommended by NIST SP 800–61 rev2, are listed here by category.

Policy structure:

1. Statement of management commitment.
2. Purpose and objectives of the policy.
3. Scope of the policy (to whom and what it applies and under what circumstances).
4. Definition of computer security incidents and related terms.
5. Organizational structure and definition of roles, responsibilities, and levels of authority.
6. Prioritization or severity ratings of incidents.
7. Performance measures.
8. Reporting and contact form. [90]

Incident response plan structure:

1. Mission.
2. Strategies and goals.
3. Senior management approval.
4. Organizational approach to incident response.

5. How the incident response team will communicate with the rest of the organization and with other organizations.

6. Metrics for measuring the incident response capability and its effectiveness.

7. Roadmap for maturing the incident response capability.

8. How the program fits into the overall organization. [90]

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- IR–1 “Incident Policies and Procedures,”
- IR–4 “Incident Handling,”
- IR–5 “Incident Monitoring,”
- IR–6 “Incident Reporting,” and
- IR–8 “Incident Response Plan.”

Related publications and resources include:

- NIST SP 800–61 rev2 “Computer Security Incident Handling Guide” and
- Chairman of the Joint Chiefs of Staff Manual on “Cyber incident handling program” (CJCSM 6510.01B).

M. ESTABLISH SECURE CONFIGURED WORKSTATION BASELINES BY IMPLEMENTING SECURITY TECHNICAL IMPLEMENTATION GUIDES

This is a *Prevention* security control.

1. Description

Computer systems, specifically workstations, as delivered by manufacturers, are typically configured from a usability perspective, rather than from a security perspective. For example, workstations might have unnecessary preinstalled software or services, have weak or even default passwords, have not installed antimalware software, etc. All these issues may make the workstation easier to use, but also increase the target surface area. A single new, improperly configured system can be used as an infiltration point by attackers.

Thus, computer systems, particularly those networked with other systems of equal or greater criticality to an organization, should be configured according to some pre-established security configuration baseline. Such baselines should be determined based on the fundamental security principles (POLP, reduce the attack surface area, etc.) using publicly developed, vetted, and supported configuration guides. Such baselines should describe the hardened profile of the operating system, and of any applications installed. A securely configured system should then be imaged and stored on a hidden logical disk drive or separate media. Typically the baseline image is used when a new workstation is put in place or for re-imaging of new workstations, or when an existing system is, or is expected to be, compromised.

2. Justification

This subsection indicates the position of similar security controls in other top-lists and provides justification for selecting this security control based on its ROI.

a. Position of Similar Security Control in the Industry Recommended "Top-lists"

- **3rd** position in the "The CIS Critical Security Controls for Effective Cyber Defense" (SANS CIS).
- **5th** position "Strategies to Mitigate Targeted Cyber Intrusions" (ASCS).
- **7th** position in the "IAD's Top 10 Information Mitigation Assurance Strategies" (NSA IAD).
- **2nd** position in the "10 Steps to Cyber Security" (UK NCSC).
- **Not included** in the "10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks" (Water-ISAC SIC, ICS-CERT, FBI).

b. Return

From a preventive perspective, enforcement of fundamental security techniques can close avenues of attack for many threats. The Defense Information Systems Agency (DISA) maintains case studies that show that the implementation of security configurations and hardening techniques can have an outstanding effect on security. For instance, DISA internal analysis claims that “over 96% of cyber incidents could have been prevented if STIGS were applied” [91]. This is a rather profound statistic, and is indicative of a very large “R” numerator in the ROI calculus used to determine the “best” security controls for rapid improvement to an organization’s security posture.

An imaged system can be very handy when preventive controls fail. For example, when an attacker has gained a root-level access, the whole system should be reimaged to the securely configured (i.e., “STIG’ed”) clean version. Having such images ready, would make this procedure relatively easy and fast to complete. Additionally, in many cases this can be performed remotely.

c. Investment

- Initial investments—requires *no* additional equipment or software purchasing.
- Implementation time—*long* (up to two months).
- Maintenance—does not require paid subscriptions or licenses. Requires *medium* staff involvement for periodical review of baseline configurations and applying patches.
- User resistance—while implementing, the control technical personnel will likely encounter *low* user resistance.
- Personnel training—requires *no* additional training for technical personnel implementing the security control.

3. Recommendations

This security control can be implemented using commercial or free configuration tools, which provide the means to set established configurations, check the settings of operating systems and applications for compliance. Configuration management tools usually use a combination of agent-based or agentless approaches. Specific settings and configuration guidelines can be found in industry recommended standards and guides, like DISA’s Security Technical Implementation Guides (STIGs), the Center for Internet Security Benchmarks Program, and the NIST National Checklist Program, etc. The baseline-configured system should be imaged, validated, and checked for vulnerabilities.

Best practices require that baseline configurations and corresponding images should be validated and newly released patches applied to the operating system and installed applications on a regular basis. Baseline images should be stored on dedicated protected repository/back-up servers, or in offline workstations that are highly isolated from the main network. To ensure that only authorized modifications are introduced to the baselines, they should be validated with integrity checking and change management tools.

NIST SP 800–53 rev4 recommendations on policies, procedures, and implementation include:

- CM–2 “Baseline Configuration,”
- CM–3 “Configuration Change Control,”
- CM–6 “Configuration Settings,”
- CM–7 “Least Functionality,” and
- MA–4 “Nonlocal Maintenance.”

Related publications and resources include:

- NIST SP 800–128 “Guide for Security-Focused Configuration Management of Information Systems,”
- NIST SP 800–123 “Guide to General Server Security,”
- DISA Security Technical Implementation Guides, and
- NIST security configuration checklist.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE WORK

Cyber espionage campaigns as well as disruptive cyber attacks have become very powerful and covert tools used by some countries to gain strategic advantage over their opponents. Intensive usage of cyber offensive capabilities in recent geopolitical conflicts, along with the rapidly expanding cyber threats landscape, requires intensification of the development of defensive cyber capabilities. In the circumstances of an ongoing military conflict, the resources and time available for such development is very restricted. Given this situation, the question that needs answering is: Given limited resources (financial, human, and time), what are the "top 13" (or so) best security controls available to help mitigate current state-supported military cyber threats? This research set about answering that question in a methodical way.

To establish a common language and discourse, Chapter II of this work covered some of the most important concepts and practices of cyber security. Cyber security can be achieved by the implementation of multiple security controls that, together, form a multilayered, defense-in-depth based security architecture. NIST SP 800–53 rev4 was identified as our primary reference for potential security controls from which to choose. We began our selection after analyzing those security controls occurring most often among well-known industry and government security control "top-lists." Even though all of these industry-recommended security controls have the same goal, to enhance cyber security by the removal or mitigation of cyber vulnerabilities, they all have slightly different emphases, approaches, and levels of abstraction. More importantly, none of them truly considers resource restrictions (i.e., the "I" in ROI) as a primary factor for a "top" control selection.

As a model of the network to be secured we have chosen a Windows-based network with Active Directory implemented, but without any security mechanisms in place. Also we have established metrics for selection of security controls that can provide high return with low investments. As our main prioritization factor, we have selected the shortest time and least effort needed for implementation; that is, "easiest things first." As the primary result of this work, we have selected and prioritized the following 13 security controls:

1. Restrict the use of administrative privileges by implementing a group security policy.
2. Enforce a strong password policy (user accounts and emails) by implementing a group security policy.
3. Establish a basic boundary defense by deploying a network intrusion prevention system.
4. Develop basic recovery capability by performing regular backups of servers.
5. Mitigate generic exploit techniques by deploying an enhanced mitigation experience toolkit.
6. Enhance end-point security by deploying a host intrusion prevention solution.
7. Control software execution by implementing application whitelisting.
8. Establish systematic OS patching by deploying an update server.
9. Perform user activity monitoring and systematic auditing by implementing group security policies.
10. Prevent unauthorized devices from getting network access by deploying a AAA server.
11. Enhance the boundary defense by configuring access lists on both border and intra-border routers.
12. Improve incident response capability by developing an incident handling program.
13. Establish secure configured workstation baselines by implementing STIGs.

Our top 13 selected security controls are each presented in a standardized format. This standard format: a) describes the control; b) contemplates both initial/upfront and ongoing maintenance costs; c) presents a subjective analysis of the potential security return (i.e., risk reduction); and d) provides general recommendations on each control’s implementation. We acknowledge that these security controls, even when implemented perfectly, will not guarantee risk-free cyber operations. We do, however, expect that deployment of the security controls on this list will facilitate a relatively rapid establishment of a “first line of defense.” Any enterprise-level organization or country adopting these controls should enjoy the benefits of advancing their cyber security posture from near nothing to something with real defensive merit in relatively short order.

Some of the security controls presented in our “top 13” list could individually be the central topic of a separate, dedicated thesis research owing to their significant complexity. For instance, the development of an incident handling program (security control #12) could be considered for future work. This work, ideally done by another Ukrainian student, could result in the development of a cyber incident handling guide for Ukrainian military cyber defense forces. This guide could be modeled after the “Cyber Incident Handling Program” (CJCSM 6510.01B) directive drafted by the U.S. Joint Chiefs of Staff, but tailored to meet the specific Ukrainian environment. Another thesis might consider development of methodology with supportive recommendations for implementation of the security control at the 11th position of this list, “Enhance boundary defense by configuring access lists on the border and inner routers.” Each of the presented security controls is complex enough to warrant more research, but also that they require frequent updating as malicious agents are persistently working to weaken network security, degrade network services and access sensitive data.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] L. Panetta. (2011, Oct. 11). Secretary of defense speech - Lee H. Hamilton lecture. U.S. Department of Defense. [Online]. Available: http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1620

[2] The Department of Defense Cyber Strategy. (2015, Apr. 17). U.S. Department of Defense. [Online]. Available: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf

[3] JP 3–12 (R), Cyberspace Operations. (2013, Feb. 5). DTIC [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

[4] B. Obama. (2013, Feb. 12). Executive Order - Improving critical infrastructure cybersecurity [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] C. Bergmann and R. Mudge. (2011, Feb. 4). There are no boundaries in cyber space. [Online]. Available: http://www.dw.com/en/there-are-no-boundaries-in-cyber-space/a-14817437

[6] M. Smith. (2010, Feb. 17). General Sir David Richards calls for new cyber-army [Online]. Available: http://www.thesundaytimes.co.uk/sto/news/uk_news/article195193.ece

[7] NIST special publication 800–53 rev4: Security and privacy controls forfederal information systems and organizations. (2013, Apr.). NIST. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[8] P. Cornish, D. Livingstone, D. Clemente, and C. Yorke. (2010, Nov.). On cyber warfare. [Online]. Available: http://www.nsci-va.org/CyberReferenceLib/2010-11-On%20Cyber%20Warfare-Chatham%20House%20Report.pdf

[9] O. Theiler. (2011, Sep. 11). New threats: the cyber-dimension [Online]. Available: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm

[10] D. Hollis. (2011, Jan. 6). Cyberwar case study: Georgia 2008. [Online]. Available: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

[11] Stuxnet analysis. (2010, Oct. 7). ENISA [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis

[12] P. Mueller and B. Yadegari. (2012, Jul.). The Stuxnet worm [Online]. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[13] P. Paganini. (2014, Aug. 4). Analysis of the Stuxnet cyber weapon family and Dragonfly [Online]. Available: http://securityaffairs.co/wordpress/27310/security/stuxnet-cyber-weapon-family.html

[14] D. Kushner. (2013). The real story of Stuxnet. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[15] J. Lewis. (2015, Apr. 28). Operation Armageddon: Cyber espionage as a strategic component of Russian modern warfare [Online]. Available: https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/

[16] Turla: Spying tool targets governments and diplomats. (2014, Aug. 7). Symantec. [Online]. Available: https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

[17] D.E. Sanger and S. Erlanger. (2014, Mar. 8). Suspicion falls on Russia as “Snake” cyberattacks target Ukraine’s government. *New York Times* [Online]. Available: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html

[18] Uroburos - highly complex espionage software with Russian roots. (2014). G Data Software AG. [Online]. Available: https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

[19] G. de Vries. Brainy Quotes. [Online]. Available: https://www.brainyquote.com/quotes/quotes/g/gijsdevrie373225.html. Accessed Feb. 17, 2017.

[20] Minimum security requirements for federal information and information systems, FIPS Pub. 200, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Techology, Gaithersburg, MD, Mar. 2006. [Online]. Available: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[21] Risk management guide for information technology systems. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Techology, Gaithersburg, MD, Jul. 2002. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[22] Moving forward with cybersecurity and privacy. (2016). PwC. [Online]. Available: https://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

[23] J. Jenkins. (2014, Nov. 14). Risk assessment a vital step in cybersecurity program development [Online]. Available: http://searchcompliance.techtarget.com/tip/Risk-assessment-a-vital-step-in-cybersecurity-program-development

[24] Risk management framework. (n.d.). NIST. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/. Accessed Feb. 17, 2017.

[25] P. Wilson. (2015). Security market trends and predictions [Online]. Available: http://www.infosecurityeurope.com/__novadocuments/231210?v=635954653779670000

[26] Glossary of terms used in NERC reliability standards. (2017, Feb. 7). NERC. [Online]. Available: http://www.nerc.com/files/glossary_of_terms.pdf. Accessed Feb. 17, 2017.

[27] A. Kim, M. H. Kang, J. Z. Luo, and A. Velasquez. (2014, Jul.). A framework for event prioritization in cyber network defense. NRL/MR/5540-14-9541, Center for High Assurance Computer Systems, Information Techology Division, Naval Research Laboratory, Washington, DC. [Online]. Available: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA608707

[28] K. Kessinger. (2015). 2015 Global cybersecurity status report [Online]. Available: https://www.isaca.org/pages/cybersecurity-global-status-report.aspx

[29] 2015 cyberthreat defense report. (2015). CyberEdge Group. [Online]. Available: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/2015-cyberthreat-defense-report-north-america-and-europe.pdf

[30] J. LaPiedra. (n.d.). The information security process [Online]. Available: https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197. Accessed Feb. 17, 2017.

[31] R. L. Kugler. (n.d.). Deterrence of cyber attacks [Online]. Available: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf. Accessed Feb. 17, 2017.

[32] R. O'Hanley and J. S. Tiller, *Information Security Management Handbook,* Boca Raton, Florida: Auerbach Publications, 2013.

[33] K. Scarfone and P. Mell. (2007, Feb.). NIST special publication 800–94: Guide to intrusion detection and prevention systems (IDPS) [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[34] FIPS publication 199: Standards for security categorization of federal information and information systems. (2004, Feb.). NIST. [Online]. Available: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[35] G. Sivathanu, C. P. Wright, and E. Zadok. (2005, Nov. 14). Ensuring data integrity in storage: Techniques and applications [Online]. Available: https://www.fsl.cs.sunysb.edu/docs/integrity-storagess05/integrity.html

[36] J. Fulp, *CS3690 Network Security*, Monterey, CA: Naval Postgraduate School, 2014.

[37] P. K. Manadhata, K. M. C. Tan, R.A. Maxion, and J.M. Wing. (2007, Aug.). An approach to measuring a system's attack surface. [Online]. Available: http://www.cs.cmu.edu/~wing/publications/CMU-CS-07-146.pdf

[38] M. Gregg, CASP CompTIA advanced security practitioner study guide: Exam CAS-002, Sybex, 2014.

[39] M. Swanson and B. Guttman. (1996, Sep.). Generally accepted principles and practices for securing information technology systems. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[40] G. McGraw and J. Viega. (2000, Oct.). Software security principles. [Online]. Available: http://www-106.ibm.com/developerworks/security/library/spriv.html?dwzone=security

[41] M. Gegick and S. Barnum. (2013, May 10). Least privilege. [Online]. Available: https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege

[42] I. N.Alateeq. (2005, Jan. 8). Design secure network segmentation approach [Online]. Available: https://www.sans.org/reading-room/whitepapers/hsoffice/design-secure-network-segmentation-approach-1645

[43] DNS Amplification Attacks. (2016, Oct. 19). US-CERT. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA13-088A

[44] J. Fulp, *CS3690 DNS-Amplification attack Q&A*, Monterey: Naval Postgraduate School, 2014.

[45] K. Vajanapoom, D. Tipper, and S. Akavipat. (n.d.). A risk management approach to resilient network design [Online]. Available: http://www.pitt.edu/~dtipper/2011/RiskPaper.pdf

[46] Koutsouris Charalampos, Marinos Louis. (2009, Dec.). Network resilience and security: challenges and measures [Online]. Available: http://akgul.bilkent.edu.tr/enisa/VWG-NetworkProvidersChallengesMeasures.pdf

[47] Defeating DDoS attacks. A Riverhead Networks Whitepaper. Riverhead Networks. [Online]. Available: http://www.cse.msu.edu/~cse825/Riverhead_WP.pdf. Accessed Feb. 20, 2017.

[48] S. Evans. (2016, Sep. 22). Krebs website Hit By 620 Gbps DDoS Attack. Infosecurity [Online]. Available: https://www.infosecurity-magazine.com/news/krebs-website-hit-by-620-gbps-ddos/

[49] B. Schneier. (2016, Sep. 13). Someone is learning how to take down the Internet [Online]. Available: https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

[50] Defeating DDOS Attacks. (2014, Jan. 23). Cisco. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html

[51] SSAC advisory SAC008: DNS distributed denial of service (DDoS) attacks. (2006). SSAC. [Online]. Available: https://www.icann.org/en/system/files/files/dns-ddos-advisory-31mar06-en.pdf

[52] A. Botchkarev and P. Andru, A return on investment as a metric for evaluating information systems: taxonomy and application. *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 6, p. 245, 2011.

[53] J. Lewis. (2013). Raising the bar for cybersecurity [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

[54] Total cost of ownership (TCO). (n.d.). Gartner. [Online]. Available: http://www.gartner.com/it-glossary/total-cost-of-ownership-tco/. Accessed Feb. 20, 2017.

[55] Understanding technology costs. (n.d.). Network Alliance. [Online]. Available: http://www.networkalliance.com/your-advantage/understanding-technology-costs. Accessed Feb. 20, 2017.

[56] CIS controls for effective cyber defense. (n.d.). Center for Internet Security. [Online]. Available: https://www.cisecurity.org/critical-controls/. Accessed Feb. 20, 2017.

[57] Strategies to Mitigate Cyber Security Incidents. (2017, Feb.). Australian government Cyber Security Operations Centre. [Online]. Available: https://www.asd.gov.au/infosec/mitigationstrategies.htm

[58] 10 steps to cyber security. (2015, Jan. 16). Communications-Electronics Security Group. [Online]. Available: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

[59] 10 Basic cybersecurity measures. best practices to reduce exploitable weaknesses and attacks. (2015, Jun.). US-CERT. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-Water-ISAC_June2015_S508C.pdf

[60] IAD's top 10 information assurance mitigation strategies. (2016, Feb. 10). IAD. [Online]. Available: https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm

[61] Removing admin rights mitigates 97% of critical Microsoft vulnerabilities. (2015, Mar. 10). Avecto. [Online]. Available: https://www.avecto.com/news-and-events/news/removing-admin-rights-mitigates-97-of-critical-microsoft-vulnerabilities/

[62] 'Top 4' strategies to mitigate targeted cyber intrusions. (2013, Jul.). Australian government Cyber Security Operations Centre. [Online]. Available: https://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf

[63] NIST special publication 800–18 (Draft): guide to enterprise password management. (2009, Apr.). NIST. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[64] Maximum password age. (2016, Jan. 28). Microsoft. [Online]. Available: https://technet.microsoft.com/en-us/library/hh994573%28v=ws.11%29.aspx

[65] CsP: Our take on the cracked AM passwords thus far. (2015, Sep. 11). CynoSure Prime. [Online]. Available: http://cynosureprime.blogspot.com.au/2015/09/csp-our-take-on-cracked-am-passwords.html

[66] Beyond the Password: the future of account security. (2015). Lawless Research. [Online]. Available: https://www.telesign.com/wp-content/uploads/2016/06/Telesign-Report-Beyond-the-Password-June-2016-1.pdf

[67] A. Singh. (2016, Jan. 11). What Symantec's intrusion prevention system did for you in 2015. [Online]. Available: https://www.symantec.com/connect/blogs/what-symantec-s-intrusion-prevention-system-did-you-2015

[68] Next generation intrusion prevention systems test results. (2016). NSS Labs. [Online]. Available: https://www.nsslabs.com/research-advisory/library/infrastructure-security/next-generation-intrusion-prevention-system/

[69] How long do disk drives last? (2013, Nov. 13). Backblaze. [Online]. Available: https://www.backblaze.com/blog/how-long-do-disk-drives-last/

[70] Advanced data recovery: hard drive recovery and RAID data recovery services. (n.d.). Advanced Data Recovery. [Online]. Available: https://www.adrdatarecovery.com/customer_service/faqs_file/data_loss_stastics

[71] Data loss statistics. (n.d.). Boston Computing Networks. [Online]. Available: https://www.bostoncomputing.net/consultation/databackup/statistics/. Accessed Feb. 20, 2017.

[72] Backing up your system. (n.d.). Massachusetts Institute of Technology. [Online]. Available: https://ist.mit.edu/security/backup. Accessed Feb. 20, 2017.

[73] T. Rains. (2012, Aug. 8). Microsoft’s free security tools – enhanced mitigation experience toolkit [Online]. Available: https://blogs.microsoft.com/microsoftsecure/2012/08/08/microsofts-free-security-tools-enhanced-mitigation-experience-toolkit/. Accessed Feb. 20, 2017.

[74] M. Stone, C. Irrechukwu, H. Perper, D.Wynne, and L. Kauffman. (2015, Oct.). NIST special publication 1800–5 (Draft): IT asset management practice guide. [Online]. Available: https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5b-draft.pdf.

[75] P. Firstbrook. (2014, Oct. 13). Market guide for application control solutions [Online]. Available: http://www.gartner.com/technology/media-products/newsletters/bit9/1-24XBRHG/gartner.html

[76] M. Souppaya and K. Scarfone. (2013, Jul). NIST special publication 800–40 revision 3: guide to enterprise patch management technologies. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[77] Update management process. (2007, Jun. 1). Microsoft. [Online]. Available: https://technet.microsoft.com/ru-ru/en%E2%80%90us/library/cc700845.aspx

[78] Critical control 4: continuous vulnerability assessment and remediation. (n.d.). SANS. [Online]. Available: http://critical-security-controls.blogspot.com/p/blog-page_4942.html.

[79] CVE Details. (2017, Jan. 23). MITRE. [Online]. Available: http://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26.

[80] Grand Theft Data. (2015). McAfee. [Online]. Available: https://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf

[81] M. Hardy. (2013, Apr.). The critical security controls: what’s NAC got to do with IT? [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-what-039-s-nac-it-35115

[82] What’s the business value and IT impact of visibility and control? (n.d.). ForeScout. [Online]. Available: https://www.forescout.com/idc-business-value/. Accessed Feb. 21, 2017.

[83] C. Boscolo. (n.d.). How to implement network access control [Online]. Available: http://www.computerweekly.com/opinion/How-to-implement-network-access-control. Accessed Feb. 21, 2017.

[84] A Cisco guide to defending against distributed denial of service attacks. (n.d.). Cisco. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html. Accessed Feb. 21, 2017.

[85] N. Navato. (2001). Easy steps to Cisco extended access list [Online]. Available: https://www.sans.org/reading-room/whitepapers/networkdevs/easy-steps-cisco-extended-access-list-231

[86] 10 Steps: incident management. (2016, Aug. 08). National Cyber Security Centre. [Online]. Available: https://www.ncsc.gov.uk/guidance/10-steps-incident-management

[87] A. Cartlidge, A. Hanna, C. Rudd, I. Macfarlane, J. Windebank, and S.Rance. (2007). An introductory overview of ITIL V3. [Online]. Available: http://www.itilnews.com/uploaded_files/itSMF_ITILV3_Intro_Overview.pdf

[88] Chairman of the Joint Chiefs of Staff Manual: cyber incident handling program. (2012, Jul 10). DTIC. [Online]. Available: http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

[89] Understanding ITIL. (2008, Aug. 25). Blogpost. [Online]. Available: http://understanding-itil.blogspot.com/

[90] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. (2012, Aug). NIST special publication 800–61 rev2: computer security incident handling guide [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[91] C. McKinney. (2016, Apr. 21). Security standards: getting the protections in place [Online]. Available: http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/3-McKinney_Security%20Standards.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California